



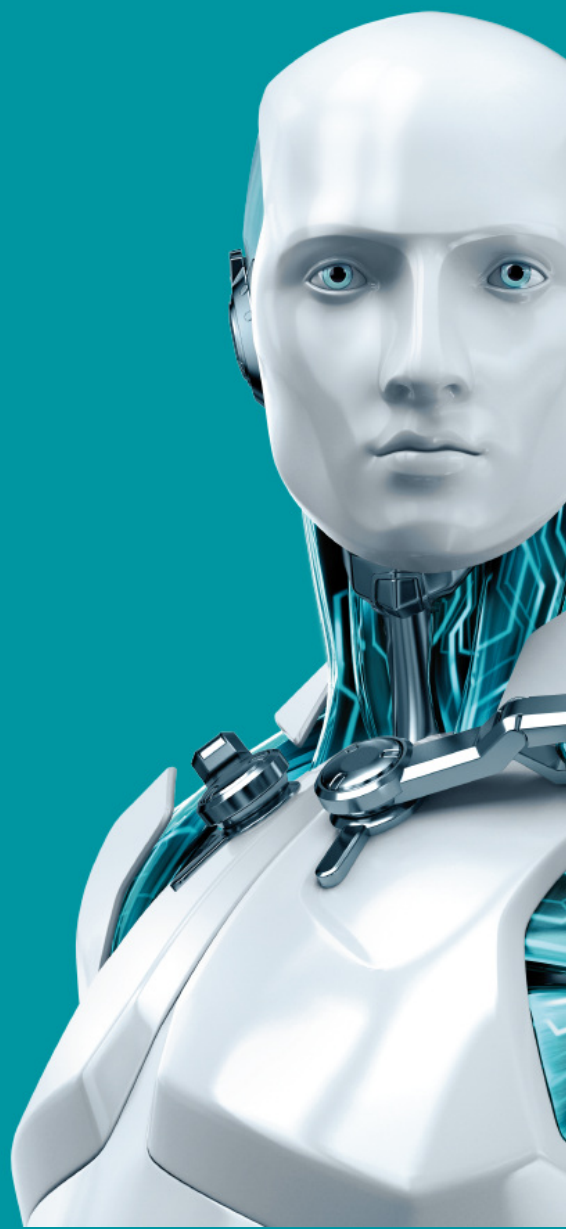
CYBER SECURITY

UŽIVATELSKÁ PŘÍRUČKA

(platná pro produkt ve verzi 6.5 a novější)

[Klikněte sem pro stažení nejnovější verze příručky](#)

ENJOY SAFER TECHNOLOGY™





© **ESET, spol. s r.o.**

ESET Cyber Security byl vyvinut společností ESET, spol. s r.o.

Pro více informací navštivte www.eset.cz.

Všechna práva vyhrazena. Žádná část této publikace nesmí být reprodukována žádným prostředkem, ani distribuována jakýmkoliv způsobem bez předchozího písemného povolení společnosti ESET, spol. s r.o.

ESET, spol. s r. o. si vyhrazuje právo změny programových produktů popsaných v této publikaci bez předchozího upozornění.

Technická podpora: www.eset.cz/podpora

REV. 13.10.2017

Obsah

1. ESET Cyber Security	5
1.1 Co je nového ve verzi 6?	5
1.2 Systémové požadavky	5
2. Instalace	6
2.1 Typická instalace	6
2.2 Pokročilá instalace	7
3. Aktivace produktu	8
4. Odinstalace	9
5. Základní přehled	10
5.1 Klávesové zkratky	10
5.2 Kontrola stavu systému	11
5.3 Co dělat, když program nepracuje správně?	11
6. Ochrana počítače	12
6.1 Antivirus a antispyware	12
6.1.1 Hlavní	12
6.1.1.1 Výjimky	12
6.1.2 Kontrola po startu	12
6.1.3 Rezidentní ochrana souborového systému	13
6.1.3.1 Rozšířené nastavení	13
6.1.3.2 Konfigurace rezidentní ochrany	13
6.1.3.3 Ověření stavu rezidentní ochrany	14
6.1.3.4 Nefunkční rezidentní ochrana?	14
6.1.4 Kontrola počítače	15
6.1.4.1 Typ kontroly	15
6.1.4.1.1 Smart kontrola	15
6.1.4.1.2 Volitelná kontrola	16
6.1.4.2 Cíle kontroly	16
6.1.4.3 Profily kontroly	16
6.1.5 Nastavení parametrů jádra ThreatSense	17
6.1.5.1 Objekty	17
6.1.5.2 Možnosti	17
6.1.5.3 Léčení	17
6.1.5.4 Přípony	18
6.1.5.5 Omezení	18
6.1.5.6 Ostatní	18
6.1.6 Zachycení infiltrace	18
6.2 Kontrola a blokování výměnných médií	19
7. Anti-Phishing	20
8. Web a mail	21
8.1 Ochrana přístupu na web	21
8.1.1 Porty	21
8.1.2 Seznam URL adres	21
8.2 Ochrana poštovních klientů	21
8.2.1 Kontrola protokolu POP3	22
8.2.2 Kontrola protokolu IMAP	22
9. Aktualizace	23
9.1 Nastavení aktualizace	23
9.1.1 Rozšířená nastavení	23
9.2 Jak vytvořit aktualizací úlohu	23
9.3 Aktualizace ESET Cyber Security na novou verzi	24
9.4 Aktualizace operačního systému	24
10. Nástroje	25
10.1 Protokoly	25
10.1.1 Údržba protokolů	25
10.1.2 Filtrování protokolů	25
10.2 Plánovač	26
10.2.1 Vytvoření nové úlohy	26
10.2.2 Vytvoření uživatelské úlohy	27
10.3 Karanténa	27
10.3.1 Vložení do karantény	27
10.3.2 Obnovení z karantény	27
10.3.3 Odesílání souborů	28
10.4 Spuštěné procesy	28
10.5 ESET LiveGrid®	28
10.5.1 Odesílání podezřelých souborů	29
11. Uživatelské rozhraní	30
11.1 Upozornění a události	30
11.1.1 Zobrazení upozornění	30
11.1.2 Stavy ochrany	30
11.2 Práva	31
11.3 Kontextové menu	31
12. Různé	32
12.1 Import a export nastavení	32
12.2 Nastavení proxy serveru	32
13. Slovník pojmů	33
13.1 Typy infiltrací	33
13.1.1 Viry	33
13.1.2 Červi	33
13.1.3 Trojské koně	33
13.1.4 Rootkity	34
13.1.5 Adware	34
13.1.6 Spyware	34
13.1.7 Potenciálně zneužitelné aplikace	34
13.1.8 Potenciálně nechtěné aplikace	34
13.2 Typy vzdálených útoků	35
13.2.1 DoS útoky	35
13.2.2 DNS Poisoning	35
13.2.3 Skenování portů	35

13.2.4	Desynchronizace TCP.....	35
13.2.5	SMB Relay.....	35
13.2.6	Útoky ICMP.....	36
13.3	Elektronická pošta.....	36
13.3.1	Reklamy.....	36
13.3.2	Fámy.....	36
13.3.3	Phishing.....	37
13.3.4	Rozpoznání nevyžádané pošty.....	37

1. ESET Cyber Security

ESET Cyber Security představuje nový přístup k plně integrované počítačové bezpečnosti. Nejnovější verze skenovacího jádra ThreatSense® je rychlá a přesná. Výsledkem je inteligentní systém, který neustále chrání váš počítač před škodlivými kódy a útoky.

ESET Cyber Security je komplexní bezpečnostní řešení, které nabízí výkonnou a účinnou ochranu při zachování minimálního dopadu na výkon systému. Na základě umělé inteligence a pokročilé heuristiky dokáže ESET Cyber Security proaktivně eliminovat viry, červy, trojské koně, spyware, adware, rootkity a další internetové hrozby, aniž by došlo ke zpomalení systému.

1.1 Co je nového ve verzi 6?

ESET Cyber Security verze 6 nabízí následující aktualizace a vylepšení:

- **Anti-Phishingová ochrana** – chrání vás před pokusy o získání hesla a dalších citlivých informací zablokováním přístupu na podvodné webové stránky, které se vydávají za legitimní.
- **Hlídní aktualizací systému** – ESET Cyber Security verze 6 přináší vylepšenou podporu systémových oznámení a bude vás pravidelně informovat o dostupných aktualizacích systému. Pro více informací se podívejte do kapitoly [aktualizace operačního systému](#) [24].
- **Stavy ochrany** – pomocí této možnosti můžete vypnout upozorňování na specifické stavy ochrany (například: *ochrana poštovních klientů je vypnutá, vyžadován restart systému*).
- **Kontrola médií** – zajišťuje kontrolu výměnných médií a umožňuje definovat jednotky, které chcete, resp. nechcete kontrolovat.

1.2 Systémové požadavky

Pro plynulý běh ESET Cyber Security by měl váš systém splňovat následující požadavky:

	Systémové požadavky
Architektura procesoru	Intel 32-bit, 64-bit
Operační systém	macOS 10.6 nebo novější
Paměť	300 MB
Pevný disk	Alespoň 200 MB volného místa

2. Instalace

Před spuštěním instalace ukončete všechny programy běžící na vašem počítači. ESET Cyber Security obsahuje komponenty, které mohou způsobit konflikt s antivirovými programy jiných výrobců. Proto doporučujeme ostatní bezpečnostní software před instalací produktu ESET.

Pro spuštění instalačního průvodce postupujte takto:

- Pokud instalujete z CD nebo DVD, vložte médium do mechaniky, otevřete médium z Plochy nebo okna **Finder** a dvojklikem na ikonu **Instalátor** spustíte instalaci programu.
- Pokud instalujete ze souboru staženého z webové stránky ESET, otevřete soubor a dvojklikem na ikonu **Instalátor** spustíte instalaci programu.



Před samotným zahájením instalace, instalační program nejprve automaticky ověří, zda není na webových stránkách dostupná novější verze produktu. Pokud ano, bude nabídnuta ke stažení a poté zahájena její instalace.

Po odsouhlasení licenčních podmínek vyberte požadovaný typ instalace:

- [Typická instalace](#) ⁶
- [Pokročilá instalace](#) ⁷

2.1 Typická instalace

Typická instalace nainstaluje produkt s doporučeným nastavením, které je vhodné pro většinu uživatelů. Toto nastavení zajišťuje maximální zabezpečení počítače v kombinaci s nízkými nároky na systémové prostředky.

ESET LiveGrid®

Systém včasného varování ESET LiveGrid® využívá aktuální informace z cloudu a umožňuje tak specialistům z virových laboratoří ESET udržovat ochranu před hrozbami na nejvyšší možné úrovni. Systém zasílá nové hrozby do virových laboratoří ESET, kde se tyto vzorky analyzují a zpracovávají. Pro změnu úrovně zapojení do tohoto systému a odesílání vzorků z vašeho počítače klikněte na tlačítko **Nastavit**. Pro více informací přejděte do kapitoly [ESET LiveGrid](#) ²⁸.

Potenciálně nechtěné aplikace

Dalším krokem při instalaci je konfigurace detekce **potenciálně nechtěných aplikací**. Tyto aplikace nemusí být nutně škodlivé, mohou však negativně ovlivňovat chování, stabilitu a výkon vašeho počítače. Aplikace jsou často přibaleny k legálně zakoupeným programům a nechtěnou instalaci můžete velmi lehce přehlédnout.

Pro dokončení instalace ESET Cyber Security doporučujeme provést kontrolu počítače na přítomnost škodlivého kódu. Pro spuštění kontroly přejděte v hlavním okně programu na záložku **Kontrola počítače** a vyberte možnost **Smart kontrola**. Pro více informací o volitelné kontrole počítače přejděte do kapitoly [volitelná kontrola počítače](#) ¹⁵.

2.2 Pokročilá instalace

Pokročilá instalace je určena zkušeným uživatelům, kteří chtějí během instalačního procesu měnit pokročilé nastavení.

Proxy server

Pokud pro připojení k internetu používáte proxy server, pro jeho konfiguraci vyberte možnost **Používám proxy server**. Následně do pole **Adresa** zadejte IP adresu nebo URL adresu proxy serveru. Pokud proxy vyžaduje autentifikaci, zadejte **uživatelské jméno** a **heslo**. Pokud proxy server nepoužíváte, vyberte **Nepoužívám proxy server**. Pokud nevíte, zda pro připojení k internetu používáte proxy server, vyberte možnost **Převzít nastavení ze systému**.

Oprávnění

V dalším kroku můžete definovat seznam privilegovaných uživatelů a skupin, které budou mít oprávnění k úpravě konfigurace programu. Ze seznamu na levé straně vyberte uživatele nebo skupinu a následně klikněte na tlačítko **Přidat** pro přidání uživatele do seznamu Privilegovaných uživatelů. Pokud ponecháte seznam prázdný, všichni uživatelé budou privilegováni.

ESET LiveGrid®

Systém včasného varování ESET LiveGrid® využívá aktuální informace z cloudu a umožňuje tak specialistům z virových laboratoří ESET udržovat ochranu před hrozbami na nejvyšší možné úrovni. Systém zasílá nové hrozby do virových laboratoří ESET, kde se tyto vzorky analyzují a zpracovávají. Pro změnu úrovně zapojení do tohoto systému a odesílání vzorků z vašeho počítače klikněte na tlačítko **Nastavit**. Pro více informací přejděte do kapitoly [ESET LiveGrid](#) 281®.

Potenciálně nechtěné aplikace

Dalším krokem při instalaci je konfigurace detekce **potenciálně nechtěných aplikací**. Tyto aplikace nemusí být nutně škodlivé, mohou však negativně ovlivňovat chování, stabilitu a výkon vašeho počítače. Aplikace jsou často přibaleny k legálně zakoupeným programům a nechtěnou instalaci můžete velmi lehce přehlédnout.

Po instalaci ESET Cyber Security byste měli provést kontrolu počítače na přítomnost škodlivého kódu. V hlavním okně programu klikněte na záložku **Kontrola počítače** a poté na **Smart kontrola**. Více informací o volitelné kontrole počítače naleznete v kapitole [Volitelná kontrola](#) 151.

3. Aktivace produktu

Po dokončení instalace budete vyzváni k aktivaci produktu. Pro aktivaci ESET Cyber Security klikněte na ikonu  v menu baru a vyberte možnost **Aktivovat produkt**. Produkt můžete aktivovat také v hlavním okně po kliknutí na záložku **Nápověda a podpora > Aktivovat produkt...** nebo **Domů > Aktivovat produkt**.

K dispozici jsou následující možnosti aktivace:

- **Licenční klíč** – unikátní řetězec znaků ve formátu XXXX-XXXX-XXXX-XXXX-XXXX, který slouží pro identifikaci vlastníka licence a její aktivaci.
- Pokud si chcete produkt ESET Cyber Security nejprve vyzkoušet, vyberte možnost **Zkušební licence**. Následně budete vyzváni k zadání e-mailové adresy, na kterou obdržíte zkušební údaje. Každý zákazník si může zkušební licenci aktivovat pouze jednou.
- Pokud zatím nemáte žádnou licenci, klikněte na možnost **Zakoupit licenci**. Následně budete přesměrováni na webové stránky lokálního distributora ESET.
- Pokud máte pouze klasické licenční údaje (uživatelské jméno a heslo), klikněte na možnost **Mám uživatelské jméno a heslo, co mám dělat?** Následně budete přesměrováni na online portál, na kterém si můžete licenční údaje přegenerovat a získat nový licenční klíč.

Po aktivaci produktu na záložce **Nápověda a podpora** v části **Informace o produktu a licenci** naleznete veřejné ID licence, které se používá pro identifikaci uživatele při komunikaci s technickou podporou společnosti ESET.

4. Odinstalace

Pro odinstalování ESET Cyber Security proveďte jeden z následujících kroků:

- Vložte instalační CD/DVD ESET Cyber Security do počítače, otevřete jej přímo z Plochy nebo okna **Finder** a dvakrát klikněte na ikonu **Odinstalovat**,
- Otevřete instalační soubor ESET Cyber Security (.dmg) a dvakrát klikněte na ikonu **Odinstalovat**,
- Spusťte **Finder**, otevřete složku **Aplikace**, stiskněte klávesu CTRL a klikněte na ikonu ESET Cyber Security. Z nabídky vyberte možnost **Zobrazit obsah balíčku**, otevřete složku **Contents > Helpers** a dvakrát klikněte na **Uninstaller**.

5. Základní přehled

Hlavní okno programu ESET Cyber Security je rozděleno na dvě části. Pravá část slouží k zobrazování informací, přičemž její obsah závisí na vybrané možnosti v levém menu.

Následuje popis jednotlivých záložek hlavního menu v levé části okna:

- **Domů** – v přehledné formě poskytuje informace o stavu ochrany počítače, přístupu na web a poštovních klientů,
- **Kontrola počítače** – umožňuje nastavit a spustit tzv. Smart nebo [volitelnou kontrolu počítače](#)^[15] a kontrolu výměnných médií,
- **Aktualizace** – zobrazuje informace o aktualizacích detekčních modulů,
- **Nastavení** – obsahuje možnosti nastavení ochrany počítače.
- **Nástroje** – zajišťují přístup k [Protokolům](#)^[25], [Plánovači](#)^[26], [Karanténě](#)^[27], [Běžícím procesům](#)^[28] a dalším funkcím programu.
- **Nápověda a podpora** – poskytuje přístup k nápovědě, ESET Databázi znalostí a webové stránky společnosti ESET. Dále zde můžete přímo vytvořit dotaz na technickou podporu a v dolní části okna naleznete informace o aktivaci produktu.

5.1 Klávesové zkratky

Klávesové zkratky, které můžete používat při práci s programem ESET Cyber Security:

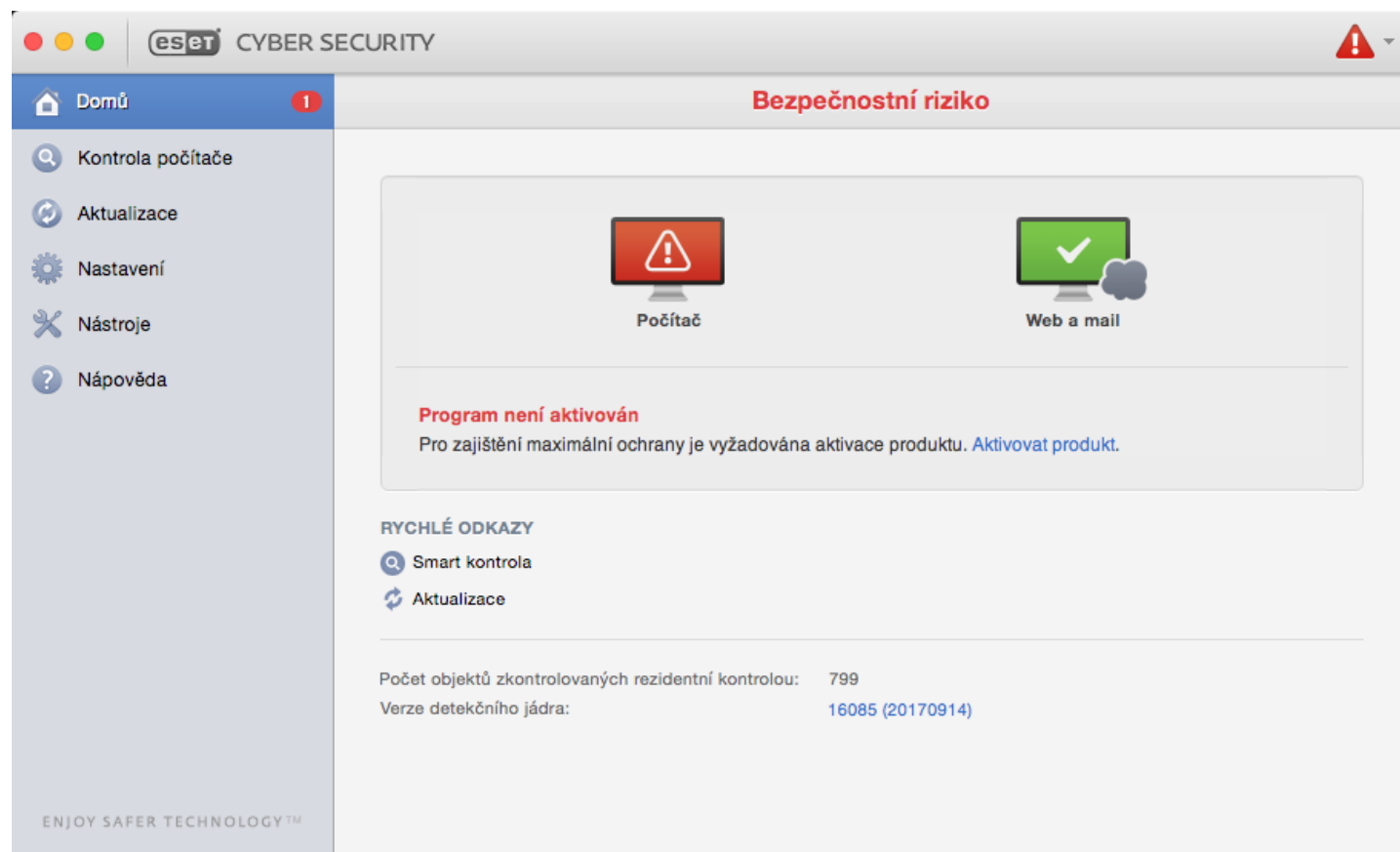
- *cmd+*, – zobrazí Rozšířené nastavení ESET Cyber Security,
- *cmd+?* – otevře nápovědou související s aktuálně otevřeným dialogovým oknem,
- *cmd+O* – obnoví výchozí pozici a velikost hlavního okna ESET Cyber Security,
- *cmd+Q* – skryje hlavní okno ESET Cyber Security. Znovu otevřít jej můžete kliknutím na ikonu  v menu baru macOS,
- *cmd+W* – zavře hlavní okno ESET Cyber Security.

Následující klávesové zkratky můžete použít pouze v případě, že máte aktivovanou možnost **Použít standardní menu**, jejíž nastavení naleznete po kliknutí v hlavním okně programu v **Nastavení > Otevřít rozšířená nastavení programu...** (nebo po stisknutí klávesy *cmd+,*) > **Rozhraní**:

- *cmd+alt+L* – otevře **Protokoly**,
- *cmd+alt+S* – otevře **Plánovač**,
- *cmd+alt+Q* – otevře **Karanténu**.

5.2 Kontrola stavu systému

Pro zjištění aktuálního stavu programu a ochrany operačního systému přejděte v hlavním menu na záložku **Stav ochrany**. V pravé části ESET Cyber Security se zobrazí stav jednotlivých modulů ochrany.



5.3 Co dělat, když program nepracuje správně?

Při plné funkčnosti ochrany má ikona stavu ochrany zelenou barvu. V opačném případě je barva červená nebo žlutá a není zajištěna maximální ochrana. Zároveň jsou na záložce **Stav ochrany** zobrazeny bližší informace o stavu jednotlivých modulů a návrh na možné řešení problému pro obnovení maximální ochrany.

Pokud uvedený návrh na řešení problému nezabral, zkuste prohledat [ESET Databázi znalostí](#) nebo kontaktujte [technickou podporu ESET](#).



6. Ochrana počítače

Nastavení počítače naleznete na záložce **Nastavení > Počítač**. Zobrazuje se zde stav **Rezidentní ochrany souborového systému a Blokování výměnných médií**. Pro vypnutí jednotlivého modulu přepněte tlačítko požadovaného modulu do stavu **VYPNUTO**. Pamatujte, že vypnutí některých modulů může snížit úroveň ochrany počítače. Pro přístup k pokročilé konfiguraci klikněte na tlačítko **Nastavit....**

6.1 Antivirus a antispyware

Antivirová ochrana chrání systém před škodlivým kódem, který by mohl provádět nechtěné změny v systému. Při detekci škodlivého kódu antivirové jádro hrozbu zablokuje, vyléčí, vymaže nebo přemístí do karantény.

6.1.1 Hlavní

V sekci **Hlavní** (dostupné v **Nastavení > Otevřít rozšířená nastavení programu... > Hlavní**) můžete nastavit detekci následujících typů aplikací:

- **Potenciálně nechtěné aplikace** – Potenciálně nechtěné aplikace jsou programy, které sice nemusí představovat bezpečnostní riziko, ale mohou mít negativní dopad na výkon počítače. Tyto aplikace se obvykle do systému nainstalují až po souhlasu uživatele. Jejich instalací dojde k určitým změnám v chování počítačového systému oproti stavu bez instalace příslušné aplikace. Mezi tyto změny v systému patří zejména zobrazování vyskakovacích (pop-up) oken, aktivace a spuštění skrytých procesů, zvýšená spotřeba systémových prostředků, změny výsledků vyhledávání a komunikace se servery výrobce aplikace.
- **Potenciálně zneužitelné aplikace** – Existuje řada legitimních programů, které za běžných podmínek zjednodušují například správu počítačových sítí. V nesprávných rukách však mohou být zneužity k nekalým účelům bez vědomí uživatele. Například se jedná o aplikace pro zobrazení vzdálené plochy a standardně je tato možnost vypnuta.
- **Podezřelé aplikace** – Jedná se o aplikace, které jsou komprimovány pomocí packerů nebo protektorů. Ty často zneužívají autoři malware, aby se vyhnuli detekci. Packery jsou runtime samorozbalovací spustitelné soubory, které spojují několik druhů škodlivého kódu do jednoho balíčku. Nejběžnějšími packery jsou UPX, PE_Compact, PKLite a ASPack. Stejný malware může být detekován odlišně, pokud je komprimován pomocí rozdílných metod. Packery navíc dokáží v průběhu času měnit své "podpisy" ve snaze vyhnout se detekci ze strany antivirových programů.

Pro vytvoření [výjimky v rezidentní a internetové ochraně](#)¹²⁾ klikněte na tlačítko **Nastavit....**

6.1.1.1 Výjimky

V této části můžete vyloučit z rezidentní ochrany soubory a složky.

Soubory a složky definované na záložce **Souborový systém** budou vyloučeny z kontroly souborů zaváděných při startu počítače, rezidentní ochrany souborového systému i volitelné kontroly počítače.

- **Cesta** – cesta k souboru nebo složce.
- **Hrozba** – pokud je vedle vyloučeného souboru zobrazen název hrozby, pak to znamená, že daný soubor je vyloučen ze skenování této konkrétní infiltrace. V případě, že je nakažen jiným druhem infiltrace, detekce proběhne.
-  – vytvoří novou výjimku. Při definování cesty k objektu můžete použít zástupné znaky (* a ?), případně konkrétní soubor nebo složku vybrat ze stromové struktury.
-  – odstraní vybranou výjimku.
- **Standardní** – odstraní všechny výjimky.

Na záložce **Web a mail** můžete vyloučit **aplikace** nebo **IP adresy** z filtrování protokolů.

6.1.2 Kontrola po startu

Standardně se provádí během startu počítače a po aktualizaci detekčních modulů kontrola souborů zaváděných při startu počítače do operační paměti. Pro změnu nastavení parametrů skenovacího jádra ThreatSense klikněte na tlačítko **Nastavení....** Více informací o nastavení ThreatSense naleznete v [této kapitole](#)¹⁷⁾.

6.1.3 Rezidentní ochrana souborového systému

Rezidentní ochrana souborového systému kontroluje všechny typy médií a spouští se při mnoha typech událostí. Využívá metody detekce technologie ThreatSense (blíže popsáno v kapitole [Nastavení parametrů skenovacího jádra ThreatSense](#)^[17]), a může se lišit pro nově vytvořené a již existující soubory. Na vytvořené soubory se může použít hlubší úroveň kontroly.

Standardně se rezidentní ochrana spouští ihned po startu a běží nepřetržitě na pozadí. V některých speciálních případech (například při konfliktu s jinými rezidentními štíty) ji můžete vypnout kliknutím na ikonu  umístěnou v menu baru a vybráním možnosti **Vypnout rezidentní ochranu souborového systému**. Rezidentní ochranu také vypnete v hlavním okně na záložce **Nastavení** > **Počítač** pomocí přepínače **ZAPNUTO/VYPNUTO** u možnosti **Rezidentní ochrana souborového systému**.

Rezidentní kontrola může kontrolovat tyto typy médií:

- **Lokální disky** – systémové pevné disky,
- **Výměnná média** – CD, DVD, USB, Bluetooth atd.
- **Síťové jednotky** – namapované síťové jednotky.

V základním nastavení se skenují soubory, ke kterým se v konkrétní chvíli přistupuje (**otevření, vytvoření nebo spuštění souboru**). Doporučujeme ponechat základní nastavení, které poskytuje maximální možnou ochranu vašeho počítače. Nastavení doporučujeme měnit pouze v ojedinělých případech, například když pozorujete zpomalení při práci s daným typem média.

Konfigurovat nastavení rezidentní ochrany můžete v Rozšířeném nastavení (dostupném po stisknutí kláves **cmd + ,** v hlavním okně programu) v sekci **Rezidentní ochrana** po kliknutí na tlačítko **Nastavit** u možnosti **Rozšířená nastavení** (blíže popsáno v kapitole [Rozšířená nastavení kontroly](#)^[13]).

6.1.3.1 Rozšířené nastavení

V tomto okně můžete definovat typy objektů kontrolované skenovacím jádrem ThreatSense. Pro více informací o kontrole samorozbalovacích archivů, runtime archivů a rozšířené heuristice přejděte do kapitoly [Nastavení parametrů skenovacího jádra ThreatSense](#)^[17].

Nedoporučujeme měnit hodnoty v sekci **Standardní nastavení archivů**, pouze v případě, že potřebujete vyřešit specifický problém jako je zpomalení rychlosti počítače při kontrole vložených archivů.

Rozšířenou heuristiku jádra ThreatSense můžete zapnout/vypnout pro kontrolu vytvářených a modifikovaných souborů a samostatně pro kontrolu spouštěných souborů. Změnu provedete pomocí možnosti **Zapnout rozšířenou heuristiku**. Rozšířená heuristika pro spouštěné soubory je standardně aktivní. Pro snížení dopadu na výkon systému doporučujeme ponechat aktivní **Smart optimalizaci** a také technologii **ESET LiveGrid**.

Zvýšit kompatibilitu se síťovými jednotkami – po aktivování této možnosti zvýšíte rychlost při přístupu k souborům umístěným na síťové jednotce. Doporučujeme ji aktivovat, pokud pozorujete zpomalení při práci se síťovými soubory. Tato funkce využívá systémový file coordinator, který je dostupný od macOS 10.10. Mějte na paměti, že file coordinator nepodporují všechny aplikace. Například Microsoft Word 2011 jej nepodporuje, zatímco Word 2016 jej podporuje.

6.1.3.2 Konfigurace rezidentní ochrany

Rezidentní ochrana patří mezi nejdůležitější součásti, pomocí kterých ESET Cyber Security pomáhá udržovat počítač zabezpečený. K úpravě parametrů rezidentní ochrany přistupujete vždy s opatrností. Tato nastavení doporučujeme upravovat pouze ve speciálních případech. Například v situaci, kdy nastane konflikt mezi produktem ESET a specifickou aplikací.

Po instalaci ESET Cyber Security, jsou všechna nastavení optimalizována pro maximální ochranu počítače. Pro obnovení nastavení na standardní hodnoty klikněte na tlačítko **Standardní** v levé části okna **Rezidentní ochrana** (dostupném po kliknutí v hlavním okně na **Nastavení** > **Otevřít rozšířená nastavení programu...** > **Ochrana** > **Rezidentní ochrana**).

6.1.3.3 Ověření stavu rezidentní ochrany

Pro ověření funkčnosti rezidentní ochrany použijte testovací soubor eicar.com. Tento soubor je speciální neškodný objekt, který detekují všechny antivirové programy. Soubor vyvinula společnost EICAR (European Institute for Computer Antivirus Research) za účelem testování antivirových programů.

Pro ověření stavu rezidentní ochrany otevřete **Terminál** a spusťte v něm následující příkaz:

```
/Applications/.esets/Contents/MacOS/esets_daemon --status
```

Stav rezidentního skeneru se zobrazí jako `RTPStatus=Enabled` nebo `RTPStatus=Disabled`.

Výstup Terminálu bude obsahovat následující informace:

- verze nainstalovaného produktu ESET Cyber Security na klientském počítači
- datum a verze aktualizace virové databáze
- cesta k aktualizacímu serveru

POZNÁMKA: Použití Terminálu doporučujeme pouze pokročilým uživatelům.

6.1.3.4 Nefunkční rezidentní ochrana?

V této kapitole jsou popsány problémové stavy, které mohou nastat při běhu rezidentní ochrany. Je zde také uvedeno jak postupovat při jejich řešení.

Rezidentní ochrana je vypnutá

Pokud byla rezidentní ochrana nedopatřením vypnuta uživatelem, je potřeba ji znovu aktivovat. Opětovné zapnutí je možné v hlavním okně programu na záložce **Nastavení** pomocí přepínače **ZAPNUTO/VYPNUTO** u možnosti **Rezidentní ochrana souborového systému**.

Rezidentní ochrana nedetekuje a neléčí infiltrace

Ujistěte se, zda nemáte nainstalován další antivirový program. Mezi dvěma rezidentními ochranami může docházet ke konfliktu. Proto doporučujeme všechny ostatní antivirové programy odinstalovat, před instalací produktu ESET.

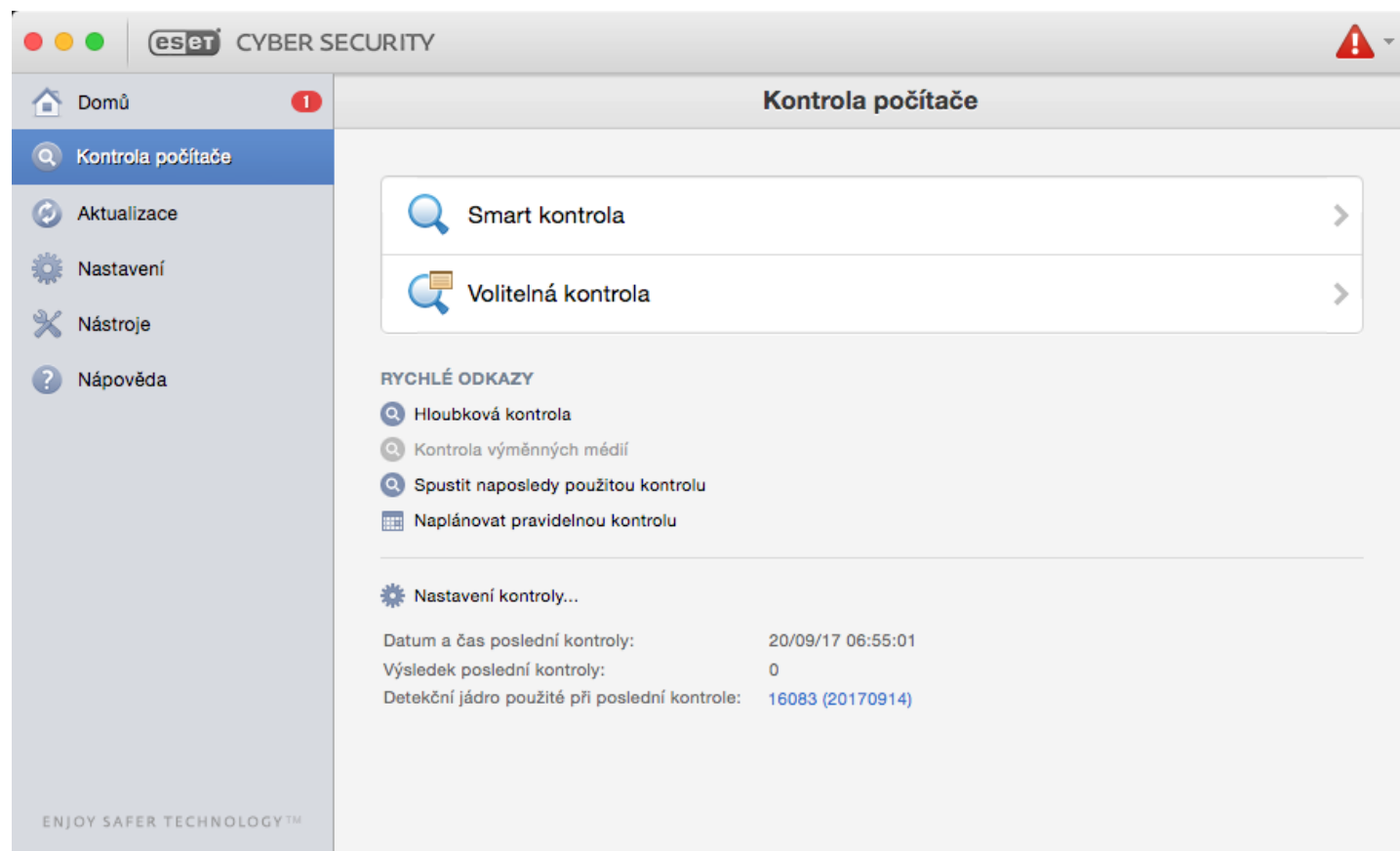
Rezidentní ochrana se nespouští při startu

Pokud se rezidentní ochrana nespouští při startu systému, zřejmě dochází ke konfliktu s jiným programem. V takovém případě doporučujeme kontaktovat technickou podporu společnosti ESET.

6.1.4 Kontrola počítače

Pokud máte podezření, že je počítač nakažen (chová se nestandardně) spusťte kontrolu počítače, v hlavním okně klikněte na **Kontrola počítače > Smart kontrola**). Pro zabezpečení maximální ochrany provádějte kontrolu počítače pravidelně, nejen při podezření na infekci. Pravidelná kontrola může odhalit infekci, která dříve prošla systémem rezidentní ochrany. To se může stát, pokud byla v některém okamžiku činnost rezidentní ochrany vypnuta, nebo nebyly aktuální detekční moduly.

Doporučujeme spouštět kontrolu počítače alespoň jednou měsíčně. Pravidelnou kontrolu můžete nastavit jako úlohu v **Plánovači** (záložka **Nástroje > Plánovač**).



Doporučujeme provádět kontrolu počítače alespoň jednou měsíčně. Pro pravidelnou kontrolu počítače můžete využít naplánované úlohy, jejichž konfiguraci naleznete v sekci **Nástroje > Plánovač**.

Soubory nebo složky, které chcete zkontrolovat můžete též uchopit myší a upustit do hlavního okna ESET Cyber Security nebo na ikonu aplikace  v menu baru, docku nebo seznamu aplikací (ve **Finderu** složka */Aplikace*).

6.1.4.1 Typ kontroly

K dispozici jsou dva druhy antivirové kontroly počítače. **Smart kontrola** rychle zkontroluje celý počítač s doporučeným nastavením kontroly. **Volitelná kontrola** umožňuje měnit parametry kontroly a také vybrat vlastní cíle (soubory, složky, média), které budou kontrolovány.

6.1.4.1.1 Smart kontrola

Smart kontrola je rychlá kontrola počítače, která léčí infikované soubory bez potřeby zásahu uživatele. Hlavní výhodou tohoto typu kontroly je její snadné použití bez nutnosti podrobného nastavování parametrů kontroly. Smart kontrola zkontroluje všechny soubory a složky a automaticky vyléčí nebo odstraní nalezené hrozby. Úroveň léčení je automaticky nastavena na standardní hodnotu. Pro podrobnější informace týkající se možností léčení si prostudujte kapitulu [Léčení](#)¹⁷.

6.1.4.1.2 Volitelná kontrola

Volitelná kontrola je vhodným řešením pokud chcete upravit všechny parametry kontroly jako jsou cíle a další nastavení. Výhodou volitelné kontroly je možnost podrobně nastavit její parametry. Různé konfigurace můžete ukládat individuálně jako uživatelské profily kontroly. To je užitečné zejména pokud potřebujete pravidelně opakovat kontrolu se stejnými parametry.

Na záložce **Kontrola počítače** > **Volitelná kontrola** můžete vybrat **Cíle kontroly** ze stromové struktury. Cíle kontroly můžete blíže specifikovat také zadáním cesty ke složce nebo k souborům. Pokud chcete vybrané cíle pouze zkontrolovat bez léčení nebo odstranění nalezených infiltrací, zaškrtněte možnost **Kontrolovat bez léčení**. Celkově si můžete vybrat ze tří úrovní léčení, po kliknutí na tlačítko **Nastavit... > Léčení**.

POZNÁMKA: Volitelnou kontrolu počítače doporučujeme zejména pokročilým uživatelům, kteří již mají předchozí zkušenost s používáním antivirových programů.

6.1.4.2 Cíle kontroly

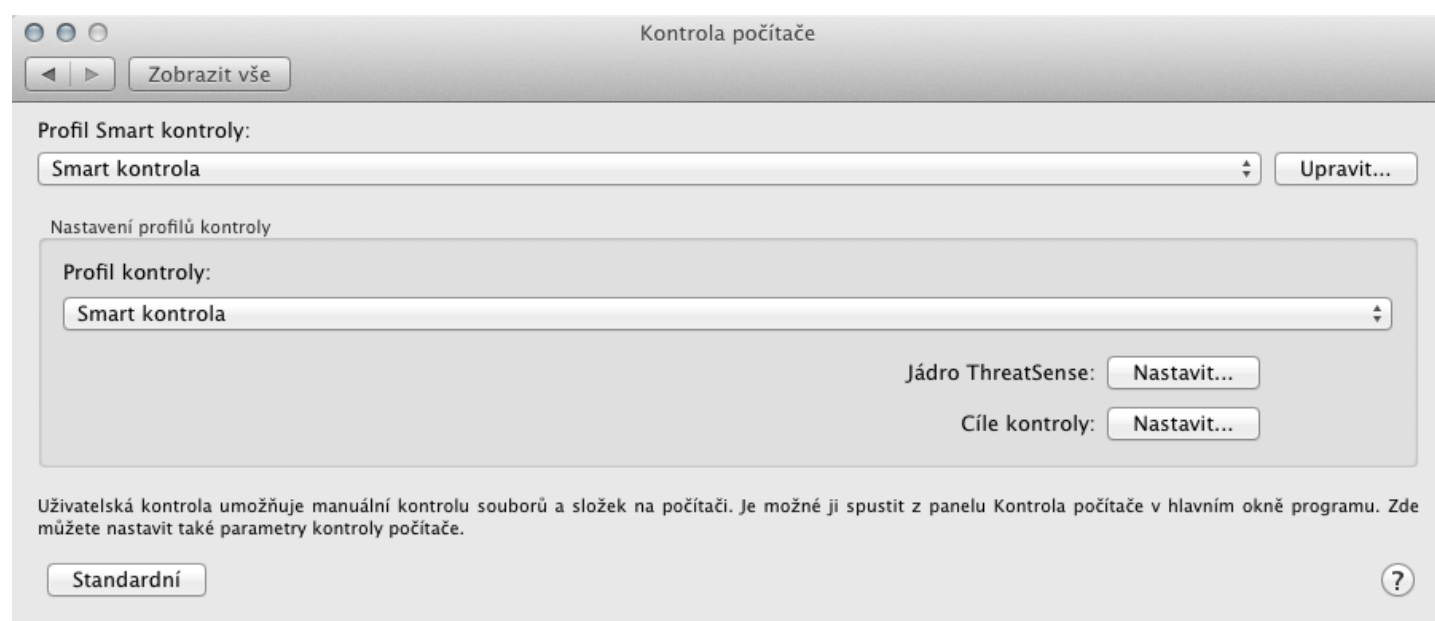
Stromová struktura cílů kontroly slouží k výběru souborů a složek, které budou zkontrolovány. Další složky mohou být automaticky vybrány z nastavení definovaném v profilu kontroly.

Cíl kontroly můžete blíže specifikovat také zadáním cesty ke složkám nebo souborům, které chcete zahrnout do kontroly. Cíle kontroly si vyberte ze stromové struktury, která obsahuje všechny složky ve vašem počítači.

6.1.4.3 Profily kontroly

Požadované nastavení kontroly si můžete uložit do profilu pro pozdější použití. Doporučujeme vytvořit nový profil (s různými cíli kontroly, metodami a dalšími parametry) pro každou pravidelně používanou kontrolu počítače.

Vytvořit nový profil můžete na záložce **Nastavení** > **Otevřít rozšířená nastavení programu...** (nebo stisknete klávesy *cmd+,*) > **Ochrana** > **Kontrola počítače** kliknutím na tlačítko **Upravit...** vedle vybraného profilu.



Podrobné informace související s vytvořením nového profilu kontroly naleznete v kapitole [Nastavení parametrů ThreatSense](#)¹⁷⁾, kde je popsáno nastavení kontroly.

Příklad: Předpokládejme, že chcete vytvořit vlastní profil kontroly a částečně Vám pro tento účel vyhovuje konfigurace Smart kontroly. Nechcete ale, aby byly kontrolovány runtime archivy a dále potřebujete nastavit přísné léčení. V okně **Seznam profilů kontroly počítače** zadejte název pro váš profil, klikněte na tlačítko **Přidat...** a potvrďte stiskem **OK**. Poté upravte parametry v nastavení **Jádra ThreatSense** a **Cíle kontroly**, tak aby odpovídaly vašim potřebám.

Pokud chcete po dokončení kontroly vypnout počítač, zaškrtněte možnost **Vypnout počítač po dokončení kontroly**.

6.1.5 Nastavení parametrů jádra ThreatSense

ThreatSense je technologie společnosti ESET, kterou tvoří soubor komplexních metod detekce infiltrací. Tato technologie je proaktivní, poskytuje tak ochranu i během prvních hodin šíření nové hrozby. K odhalení hrozeb využívá kombinaci několika metod (analýza kódu, emulace kódu, generické signatury, ...), které efektivně kombinuje a zvyšuje tím bezpečnost systému. Skenovací jádro je schopné kontrolovat několik datových toků paralelně a maximalizovat tak svůj výkon a účinnost detekce. Technologie ThreatSense dokáže účinně odstraňovat také rootkity.

Technologie ThreatSense umožňuje nastavit následující parametry kontroly:

- Typy souborů a přípony, které se mají kontrolovat,
- Kombinace různých detekčních metod,
- Úrovně léčení.

Pro otevření okna s nastavením parametrů ThreatSense klikněte v hlavním okně programu na **Nastavení > Otevřít rozšířená nastavení programu...** a následně klikněte na tlačítko **Nastavit...** a to v sekci **Ochrana systému, Rezidentní ochrana a Kontrola počítače**, které používají ThreatSense technologii. Odlišné bezpečnostní scénáře vyžadují rozdílné konfigurace. V rámci technologie ThreatSense můžete konfigurovat následující moduly:

- **Kontrola po startu** – kontrola souborů spouštěných po startu,
- **Rezidentní ochrana** – ochrana počítače v reálném čase,
- **Kontrola počítače** – kontrola složek a souborů.
- **Ochrana přístupu na web,**
- **Ochrana poštovních klientů.**

Parametry ThreatSense jsou speciálně optimalizovány pro každý modul a jejich změna může podstatně ovlivnit práci systému. Příkladem může být změna nastavení tak, aby byla vždy provedena kontrola runtime archivů, nebo zapnutí rozšířené heuristiky pro modul rezidentní ochrany souborů. Nicméně takové změny mohou způsobit celkové zpomalení systému. Proto doporučujeme ponechat původní nastavení ThreatSense beze změny. Určitou volnost v konfiguraci ponechává modul **Kontrola počítače**.

6.1.5.1 Objekty

V sekci **Objekty** můžete definovat typy souborů, které se budou kontrolovat na přítomnost infiltrace.

- **Symbolické odkazy** – (dostupné pouze pro kontrolu počítače) kontrola speciálních typů souborů, které obsahují textovou informaci s cestou k jinému souboru či složce.
- **Soubory e-mailů** – (není dostupné v rezidentní ochraně) kontrola souborů, které obsahují e-mailové zprávy.
- **Poštovní schránky** – (není dostupné v rezidentní ochraně) kontrola uživatelských poštovních účtů. Nesprávné použití může vést ke konfliktu s vaším e-mailovým klientem. Pro více informací o výhodách a nevýhodách si přečtěte [tento článek](#).
- **Archivy** – (není dostupné v rezidentní ochraně) kontrola souborů v archivech (.rar, .zip, .arj, .tar, apod.).
- **Samorozbalovací archivy** – (není dostupné v rezidentní ochraně) kontrola souborů v samorozbalovacích archivech.
- **Runtime archiv** – runtime archiv se na rozdíl od klasických archivů dekomprimují v paměti počítače po spuštění souboru (typicky UPX, ASPack, yoda, FGS, apod.).

6.1.5.2 Možnosti

V této sekci můžete vybrat metody, které se použijí při kontrole počítače na přítomnost škodlivého kódu.

- **Zapnout heuristiku** – Heuristika používá algoritmus pro analýzu (škodlivé) aktivity programů. Hlavní výhodou heuristické detekce je její schopnost identifikovat škodlivý software, který předtím neexistoval.
- **Zapnout rozšířenou heuristiku** – Rozšířená heuristika používá jedinečný algoritmus vyvinutý společností ESET, který dokáže detekovat červy a trojské koně napsané ve složitých programovacích jazycích. Schopnost detekce těchto hrozeb je tak značně vyšší právě díky rozšířené heuristice.

6.1.5.3 Léčení

Nastavení pro léčení určuje způsob jakým kontrola vyléčí infikované soubory. Léčení má tři úrovně:

- **Neléčit** – infikované soubory se automaticky nevyléčí. Program zobrazí okno s varováním a možností výběru akce,
- **Standardní úroveň léčení** – program se pokusí automaticky vyléčit, nebo vymazat infikovaný soubor. Pokud není možné provést akci automaticky, program nabídne možnost výběru akce,
- **Přísné léčení** – program vyléčí, nebo vymaže všechny infikované soubory (včetně archivů). Jedinou výjimku tvoří systémové soubory. Pokud je nelze vyléčit, program zobrazí okno s varováním s možností výběru akce.

Upozornění: V přednastaveném režimu standardní úrovně léčení je vymazán celý archiv, pouze pokud jsou všechny soubory v archivu infikované. Pokud tedy archiv obsahuje i legitimní soubory (nenapadené), nebude vymazán. Pokud je archiv detekován v režimu přísného léčení, bude tento archiv vymazán pokud obsahuje alespoň jeden soubor s infiltrací, bez ohledu na stav ostatních souborů.

6.1.5.4 Přípony

Přípona souboru je součástí jeho názvu, ve kterém je oddělena tečkou. Přípona označuje typ a obsah souboru. V této části nastavení parametrů ThreatSense můžete nastavit typy souborů, které budou kontrolovány.

Standardně se kontrolují všechny soubory bez ohledu na příponu. Do seznamu souborů vyloučených z kontroly může být přidána jakákoli přípona. Pomocí tlačítek  a  můžete povolit nebo zakázat kontrolu požadovaných souborů podle jejich přípon.

Vyloučení přípon je někdy nutné, pokud probíhající kontrola narušuje činnost specifického programu, který k daným typům souborů bude přistupovat. V některých případech může být vhodné vyloučit z kontroly soubory s příponou *.log*, *.cfg* a *.tmp*. Níže uvádíme správný formát zápisu (každá přípona je na samostatném řádku):

log
cfg
tmp

6.1.5.5 Omezení

V sekci **Omezení** nastavíte maximální velikost kontrolovaných objektů a maximální hloubku kontroly v archivech (počet vnořených archivů které budou kontrolovány).

- **Maximální velikost:** určuje největší možnou velikost souborů, které budou zkontrolovány. Modul antiviru bude kontrolovat pouze objekty s menší velikostí než je definovaná hodnota. Nedoporučujeme měnit přednastavenou hodnotu, protože většinou není pro tuto změnu důvod. Doporučujeme, aby tuto hodnotu měnili jen pokročilí uživatelé, kteří potřebují vyloučení větších objektů z kontroly.
- **Maximální čas kontroly:** upravuje maximální čas věnovaný kontrole jednoho objektu. Pokud je zde nastavena hodnota, antivirový modul přestane kontrolovat objekt po uplynutí nastavené doby, bez ohledu na to, zda byla kontrola objektu dokončena či nikoli.
- **Maximální úroveň vnoření:** upravuje maximální hloubku vnoření při kontrole archivů. Pokud nejste zkušený uživatel, nedoporučujeme vám měnit přednastavenou hodnotu 10. Za běžných okolností není důvod toto nastavení měnit. Pokud se kontrola ukončí kvůli překročení počtu úrovní vnoření archivů, celý archiv zůstane nezkontrolován.
- **Maximální velikost souboru:** umožňuje nastavit maximální reálnou velikost souborů v archivech, které budou zkontrolovány. Pokud se kontrola ukončí kvůli tomuto omezení, celý archiv zůstane nezkontrolován.

6.1.5.6 Ostatní

Zapnout Smart optimalizaci

Se zapnutou Smart optimalizací se automaticky nastaví nejvýhodnější poměr mezi efektivitou a rychlostí kontroly. Smart optimalizace spočívá v inteligentním použití různých kontrolních metod pro různé typy souborů v rámci jednotlivých modulů ochrany. Nastavení Smart optimalizace není pevně definováno a vývojářský tým společnosti ESET má možnost podle potřeby měnit moduly prostřednictvím pravidelné automatické aktualizace ESET Cyber Security. Pokud je Smart optimalizace vypnuta, aplikuje se při kontrole souborů výhradně nastavení definované uživatelem v nastaveních skenovacího jádra ThreatSense jednotlivých modulů.

Kontrolovat alternativní datové proudy (platí pouze pro kontrolu počítače)

Alternativní datové proudy (resource/data forks) používané systémem NTFS jsou běžným způsobem neviditelné asociace k souborům a složkám. Mnoho hrozeb je proto využívá pro zabránění detekce.

6.1.6 Zachycení infiltrace

Infiltrace se do systému mohou dostat mnoha způsoby: z internetových stránek, sdílených složek, pošty, výměnných médií (USB, externí disky, CD, DVD, diskety atd.).

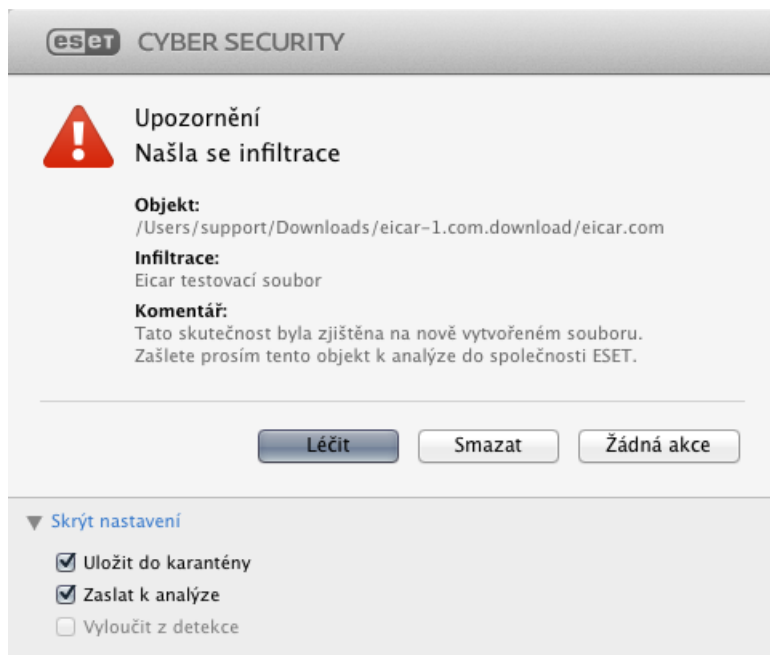
Pokud váš počítač vykazuje znaky napadení škodlivým kódem, např. je pomalejší, často "mrzne" apod., doporučujeme provést následující kroky:

1. Otevřete ESET Cyber Security a klikněte na záložku **Kontrola počítače**.
2. Vyberte **Smart kontrola** (více informací v kapitole [Smart kontrola](#) ^[15]).
3. Po dokončení kontroly, zkontrolujte zobrazený protokol.

Pokud chcete zkontrolovat pouze určitou část disku, vyberte možnost **Volitelná kontrola** a vyberte vlastní cíle kontroly.

Obecným příkladem postupu při řešení problému s infiltrací je situace, kdy rezidentní ochrana souborového systému s nastavenou standardní úrovní léčení najde hrozbu a pokusí se o vyléčení nebo vymazání souboru. Pokud modul rezidentní ochrany nemá nastavenou akci, která se má provést, požádá Vás o výběr akce prostřednictvím okna s upozorněním. Obvykle jsou k dispozici možnosti **Léčit**, **Smazat** a **Ponechat**. Pokud vyberte **Ponechat**, s infikovaným souborem se neprovede žádná akce, což nedoporučujeme. Výjimkou může být situace, kdy máte jistotu, že soubor je neškodný a byl chybně detekován.

Léčení a vymazání – použijte léčení, pokud byl soubor napaden virem, který k němu přidal škodlivý kód. Infikovaný soubor se tak může v některých případech obnovit do původního stavu. Pokud však soubor obsahuje výhradně škodlivý kód, bude vymazán.



Mazání souborů v archivech – ve výchozím režimu léčení bude celý archiv vymazán pouze tehdy, pokud obsahuje výhradně infikované a žádné "čisté" soubory. Jinými slovy, archivy se nevymazávají, pokud obsahují i neškodné (nenapadené) soubory. Opatrnost je však nutná, pokud spustíte kontrolu s nastavením **Přísné léčení** - v režimu Přísné léčení bude totiž archiv obsahující alespoň jeden soubor s infiltrací, bez ohledu na stav ostatních souborů v archivu smazán.

6.2 Kontrola a blokování výměnných médií

ESET Cyber Security nabízí volitelnou kontrolu výměnných médií po jejich vložení (CD, DVD, USB, zařízení s operačním systémem iOS a další).



Výměnná média mohou obsahovat škodlivý kód a představovat tak riziko pro počítač. Pro blokování výměnných médií klikněte na tlačítko **Nastavit...** na záložce **Nastavení > Počítač > Blokování výměnných médií** a zaškrtněte možnost **Aktivovat blokování výměnných médií**. Pro povolení konkrétních typů médií odstraňte označení u požadovaného typu média. Do nastavení se také dostanete z dialogového okna kliknutím na **Nastavení blokování médií**, které se zobrazí po vložení média do počítače, viz obrázek výše.

POZNÁMKA: Pro přístup k externím CD-ROM jednotkám připojených pomocí USB kabelu odškrtněte možnost **CD-ROM**.

7. Anti-Phishing

Termín *phishing* definuje kriminální činnost, která využívá sociální inženýrství (manipulace uživatelů za účelem získání citlivých dat). Nejčastěji se snaží získat přístup k bankovnímu účtu nebo PIN.

Důrazně doporučujeme tuto ochranu aktivovat v rozšířeném nastavení (dostupném po stisknutí kláves `cmd + ,` v hlavním okně programu) v sekci **Anti-Phishingová ochrana** > vybráním možnosti **Zapnout Anti-Phishingovou ochranu**. ESET Cyber Security poté zablokuje a zobrazí upozornění při detekování všech potenciálních phishingových útoků pocházejících z podezřelých webových stránek a domén.

8. Web a mail

Nastavení webové a mailové ochrany najdete po kliknutí v hlavním okně programu na **Nastavení > Web a Mail**. Upravit podrobné nastavení jednotlivých modulů ochrany můžete po kliknutí na tlačítko **Nastavit....**

- **Ochrana přístupu na web** – monitoruje HTTP komunikaci mezi webových prohlížečem a vzdálenými servery.
- **Ochrana poštovních klientů** – poskytuje kontrolu e-mailové komunikace přijímané pomocí POP3 a IMAP protokolu.
- **Anti-Phishingová ochrana** – blokuje potenciální útoky přicházející z webových stránek a domén zařazených v databázi ESET.

8.1 Ochrana přístupu na web

Ochrana přístupu na web monitoruje veškerou komunikaci mezi webovými prohlížeči a vzdálenými servery pomocí protokolu HTTP (Hypertext Transfer Protocol).

Ve výchozím nastavení je kontrolována komunikace na standardních portech. V případě potřeby můžete definovat [další porty](#)^[21] a případně využít [seznamy URL adres](#)^[21].

8.1.1 Porty

Na záložce **Porty** můžete definovat čísla portů, které jsou používány pro HTTP komunikaci. Standardně jsou přednastaveny porty 80, 8080 a 3128.

8.1.2 Seznam URL adres

Správa seznamů URL adres umožňuje definovat seznamy adres webových stránek, které budou blokovány, povoleny, nebo vyloučeny z kontroly. Webové stránky zařazené na seznamu blokovanych stránek nebudou dostupné, zatímco stránky vyloučené z kontroly nebudou kontrolovány na přítomnost škodlivého kódu.

Pokud chcete povolit přístup pouze na adresy uvedené v **Seznamu povolených adres**, aktivujte možnost **Povolit přístup pouze na URL adresy zařazené do seznamu povolených adres**.

Pro aktivování daného seznamu aktivujte možnost **Seznam je aktivní**. Pokud chcete zobrazit upozornění při přístupu na webovou stránku umístěnou na seznamu, zaškrtněte možnost **Upozornit při aplikování adresy ze seznamu**.

V seznamech můžete používat speciální znaky * a ?. Přičemž znak * nahrazuje libovolný řetězec a znak ? nahrazuje libovolný znak. Vyloučené adresy se nekontrolují proti hrozbám a proto by měl seznam výjimek obsahovat pouze ověřené a důvěryhodné adresy. Rovněž je potřeba dbát opatrnosti při používání speciálních znaků v tomto seznamu.

8.2 Ochrana poštovních klientů

Ochrana poštovních klientů zabezpečuje kontrolu poštovní komunikace přijímané prostřednictvím protokolu POP3 a IMAP. Při kontrole přijímaných zpráv jsou použity všechny pokročilé metody obsažené ve skenovacím jádře ThreatSense. Kontrola POP3 a IMAP protokolu je nezávislá na typu poštovního klienta. Nastavení tohoto modulu najdete na záložce **Nastavení > Ochrana poštovních klientů**.

Jádro ThreatSense – pokročilé nastavení kontroly poštovních klientů jako jsou cíle kontroly, metody detekce atd. Pro zobrazení nastavení klikněte na tlačítko **Nastavit....**

ESET Cyber Security umožňuje do kontrolovaných zpráv přidávat podpis s informacemi o výsledku kontroly, po aktivování možnosti **Přidávat upozornění do předmětu zpráv**). Tato informace však není spolehlivá, jelikož některé zprávy mohou být škodlivým kódem pozměněny. Možná nastavení jsou následující:

- **Nikdy** – podpisy nebudou přidávány do žádných kontrolovaných zpráv,
- **Pouze do infikovaných zpráv** – podpisy budou přidávány pouze do infikovaných zpráv,
- **Do všech kontrolovaných zpráv** – podpisy budou přidávány do všech kontrolovaných zpráv.

Šablona přidávaná do předmětu infikovaných zpráv – prefix, který bude přidán do předmětu infikovaných zpráv.

Přidávat upozornění do poznámky pod čarou – přidá informaci o nákaze do infikovaných zpráv. Pomocí této funkce můžete snadno filtrovat zprávy s nákazou.

Dále se můžete rozhodnout, zda chcete aby byly kontrolovány zprávy při jejich příjmu, resp. odesílání. Více informací naleznete v kapitole:

- [Kontrola protokolu POP3](#)^[22]
- [Kontrola protokolu IMAP](#)^[22]

8.2.1 Kontrola protokolu POP3

POP3 protokol je nejrozšířenější protokol pro příjem e-mailové komunikace prostřednictvím poštovního klienta. ESET Cyber Security zabezpečuje ochranu tohoto protokolu nezávisle na používaném poštovním klientovi.

Modul zabezpečující kontrolu se zavádí při startu operačního systému a po celou dobu je zaveden v paměti. Pro správné fungování stačí ověřit, zda je modul zapnutý. Kontrola POP3 protokolu je prováděna automaticky bez nutnosti konfigurace poštovního klienta. Standardně je kontrolována komunikace na portu 110. V případě potřeby můžete přidat také další používané porty, kdy čísla portů oddělujete čárkou.

Aktivovat kontrolu protokolu POP3 – zapne kontrolu poštovní komunikace přes POP3 na přítomnost škodlivého kódu.

8.2.2 Kontrola protokolu IMAP

IMAP (Internet Message Access Protocol) je další internetový protokol pro přijímání e-mailových zpráv. IMAP má v porovnání s protokolem POP3 několik výhod. Umožňuje například připojení více klientů na stejný účet a zachovávání informace stavu zprávy (zda zpráva byla či nebyla přečtena, bylo na ni odpovězeno nebo byla vymazána). ESET Cyber Security zabezpečuje ochranu tohoto protokolu nezávisle na používaném poštovním klientovi.

Modul zabezpečující kontrolu se zavádí při startu operačního systému a po celou dobu je zaveden v paměti. Pro správné fungování stačí ověřit, zda je modul zapnutý. Kontrola IMAP protokolu je prováděna automaticky bez nutnosti konfigurace poštovního klienta. Standardně je kontrolována komunikace na portu 143. V případě potřeby můžete přidat také další používané porty, kdy čísla portů oddělujete čárkou.

Aktivovat kontrolu protokolu IMAP – zapne kontrolu poštovní komunikace přes IMAP na přítomnost škodlivého kódu.

9. Aktualizace

Pravidelná aktualizace ESET Cyber Security je základním předpokladem pro zajištění maximální bezpečnosti systému. Modul Aktualizace se stará o to, aby byl program stále aktuální pomocí aktualizace detekčních i programových modulů.

Informace o aktuálním stavu aktualizace se zobrazují na záložce **Aktualizace** v hlavním okně programu. Obsahují informaci o datu a čase poslední úspěšné aktualizace, zda jsou moduly aktuální, případně jestli není potřeba program aktualizovat. Kliknutím na **Aktualizovat moduly** spustíte aktualizaci ručně.

Pokud jsou moduly v pořádku staženy a aktuální, zobrazuje se informace **Aktualizace není potřeba - moduly jsou aktuální**. Pokud nelze program aktualizovat, zkontrolujte [Nastavení aktualizace](#)^[23]. Nejčastější příčinou selhání stahování aktualizací je [neaktivovaný produkt](#), případně chybně nastavený [proxy server](#)^[32].

Záložka Aktualizace v hlavním okně programu obsahuje také číselné označení detekčního jádra. Jedná se zároveň o funkční odkaz vedoucí na webové stránky společnosti ESET s podrobnými informacemi o nových verzích, které aktualizace zahrnuje.

9.1 Nastavení aktualizace

Pro odstranění všech dočasně uložených aktualizacích souborů klikněte na tlačítko **Vyčistit** v dialogovém okně **Aktualizace**. Vymazat dočasné soubory doporučujeme provést v případě problémů s aktualizací.

Pokud potřebujete konfigurovat podrobně způsob aktualizace, nastavit používání proxy atp., klikněte na tlačítko **Nastavit....**

9.1.1 Rozšířená nastavení

Pro deaktivaci zobrazování upozornění o provedené aktualizaci modulů aktivujte možnost **Nezobrazovat upozornění o úspěšné aktualizaci**.

Pokud chcete mít přístup k vývojářským aktualizacím, které mohou řešit váš problém, aktivujte si stahování **testovacích aktualizací**. Vyberete-li možnost **Opožděná aktualizace**, aktualizace se budou stahovat z aktualizacího severu, na který jsou aktualizace umísťovány se zpožděním (o několik hodin). Výhodou je stahování ověřených aktualizací, které nezpůsobují problémy, ale zároveň se tím snižuje úroveň zabezpečení.

ESET Cyber Security zálohuje detekční a programové moduly pro případ obnovení starší verze. Aby se obrazy tzv. snapshoty modulů vytvářely, ponechte možnost **Vytvářet zálohu aktualizacích souborů** zaškrtnutou. **Počet vytvářených záloh** určuje počet obrazů předchozích modulů uložených na lokálním disku počítače. Pokud chcete vrátit předchozí aktualizaci, nejprve pomocí rozbalovacího menu **Pozastavit aktualizace** na vyberte dobu, na kterou chcete pozastavit stahování aktualizací, a poté klikněte na tlačítko **Vrátit předchozí aktualizace**. Vyberte možnost **Do odvolání**, pokud chcete stahování aktualizací obnovit ručně kliknutím na tlačítko **Povolit aktualizace**. Protože tato možnost představuje potenciální bezpečnostní riziko, její výběr nedoporučujeme.

Nastavit automaticky maximální stáří databáze – pomocí této možnosti nastavíte maximální přístupné stáří detekčních modulů. Budou-li starší, zobrazí se informace, že moduly nejsou aktuální. Předdefinovaná doporučená hodnota je 7 dní.

9.2 Jak vytvořit aktualizací úlohu

Aktualizaci můžete spustit kdykoliv ručně kliknutím na **Aktualizovat moduly** na záložce **Aktualizace** v hlavním okně ESET Cyber Security.

Aktualizaci můžete také spouštět jako naplánovanou úlohu. Pro vytvoření naplánované úlohy klikněte v hlavním okně programu na záložku **Nástroje > Plánovač**. Standardně jsou v ESET Cyber Security již vytvořeny tyto aktualizací úlohy:

- **Pravidelná automatická aktualizace,**
- **Automatická aktualizace po přihlášení uživatele.**

Každá z těchto úloh může být nastavena tak, aby odpovídala vašim potřebám. Kromě úpravy stávajících úloh aktualizace můžete vytvářet i nové úlohy s vlastní konfigurací. Pro bližší popis vytváření a nastavení úloh přejděte do kapitoly [Plánovač](#)^[26].

9.3 Aktualizace ESET Cyber Security na novou verzi

Pro zaručení maximální ochrany před škodlivým kódem je důležité vždy používat (mít nainstalovanou) nejnovější verzi produktu ESET Cyber Security. Pro ověření dostupnosti nové verze produktu přejděte v hlavním okně programu na záložku **Domů**. Jakmile bude dostupná nová verze, zobrazí se na této záložce upozornění. Kliknutím na **Zjistit více...** zobrazíte informace o nové verzi programu včetně čísla verze a seznamu změn.

Kliknutím na tlačítko **Ano** zahájíte stahování nejnovější verze, případně aktualizaci odložíte na později kliknutím na **Nyní ne**.

Po odsouhlasení aktualizace produktu se instalační soubor stáhne do složky stažených souborů, případně jiné složky nastavené v internetovém prohlížeči. Po dokončení stahování soubor spusťte a postupujte podle kroků instalačního průvodce. Vaše licenční údaje (uživatelské jméno a heslo) a nastavení budou automaticky přeneseny do nové instalace. Dostupnost nové verze produktu doporučujeme pravidelně kontrolovat, zejména v případě, když jste instalovali ESET Cyber Security z CD nebo DVD.

9.4 Aktualizace operačního systému

Aktualizace systému macOS představují důležitou součást v ochraně proti škodlivému software. Pro maximální bezpečnost doporučujeme instalovat aktualizace co nejdříve po jejich vydání. ESET Cyber Security vás může upozornit na chybějící aktualizace systému v závislosti na nastavené úrovni. Po kliknutí v hlavním okně na **Nastavení > Zobrazit rozšířené nastavení...** (nebo stisknutím kláves `cmd+,`) > **Upozornění a události > Nastavení...** můžete změnit následující **Podmínky upozornění** v sekci **Aktualizace operačního systému**:

- **Zobrazit všechny aktualizace** – budete upozorněni pouze na instalaci všech aktualizací operačního systému
- **Zobrazit pouze doporučené** – budete upozorněni pouze na instalaci důležitých aktualizací operačního systému.

Pokud nechcete být informováni o chybějících aktualizacích systému, odškrtněte možnost **Aktualizace operačního systému**.

Informace o dostupnosti aktualizací operačního systému macOS a souvisejících aplikací jsou poskytovány systémovým nástrojem Aktualizace systému. Aktualizaci můžete spustit přímo ze zobrazeného okna nebo kliknutím na záložku **Domů** v hlavním okně ESET Cyber Security na **Instalovat chybějící aktualizace**.

Okno s upozorněním obsahuje název aplikace, verzi, velikost aktualizace, vlastnosti (vlajky) a další informace o aktualizaci. Sloupec **Vlajky** může obsahovat následující informace:

- **[doporučeno]** – výrobce operačního systému doporučuje nainstalovat tuto aktualizaci pro zvýšení bezpečnosti a stability operačního systému,
- **[restart]** – po dokončení instalace je vyžadován restart,
- **[vypnutí]** – po dokončení instalace bude nutné vypnout a znovu zapnout počítač.

Okno s upozorněním zobrazuje aktualizace získané pomocí nástroje 'softwareupdate'. Aktualizace získané pomocí tohoto nástroje se mohou lišit od seznamu aktualizací poskytovaných pomocí aplikace 'Aktualizace aplikací.' Pokud chcete nainstalovat aktualizace zobrazené v okně 'Chybějící aktualizace systému' a aplikace 'Aktualizace aplikací' je nezobrazuje, je nutné použít nástroje 'softwareupdate' z příkazového řádku. Pro více informací o nástroji 'softwareupdate' se podívejte do manuálu po zadání `man softwareupdate` do okna **Terminál**. Toto doporučujeme pouze zkušeným uživatelům.

10. Nástroje

Záložka **Nástroje** obsahuje nástroje, které pomáhají zjednodušit správu programu a nabízí dodatečné možnosti pro zkušené uživatele.

10.1 Protokoly

Protokoly zachycují všechny podstatné události programu a nabízejí přehled detekovaných hrozeb. Záznamy v protokolech představují důležitý nástroj pro systémové analýzy, detekci hrozeb a řešení problémů. Vytváření protokolů probíhá aktivně na pozadí bez jakékoli interakce s uživatelem. Informace se zaznamenávají podle aktuálních nastavení podrobnosti protokolů. Textové informace a protokoly si můžete prohlédnout i archivovat přímo v prostředí ESET Cyber Security.

Protokoly jsou dostupné v hlavním menu ESET Cyber Security na záložce **Nástroje > Protokoly**. Požadovaný typ protokolu vyberte z rozbalovacího menu **Protokol** v horní části okna. Dostupné jsou následující typy protokolů:

1. **Zachycené infiltrace** – tento protokol je vhodné použít k prohlížení všech událostí týkajících se detekce infiltrací,
2. **Události** – všechny důležité akce, které provede ESET Cyber Security jsou zaznamenány v tomto protokolu. Tento protokol je určen hlavně správcům systémů a uživatelům při řešení různých problémů,
3. **Kontrola počítače** – výsledky každé kontroly počítače se zobrazují v tomto protokolu. Kliknutím na položku v protokolu zobrazíte podrobnosti vybrané kontroly počítače,
4. **Filtrované webové stránky** – tento seznam je užitečný v případě, že si chcete prohlédnout stránky blokované modulem ochrana přístupu na web. Protokol obsahuje informace o času, URL adrese, uživateli a aplikaci, která se chtěla na stránky připojit.

Jednotlivé události v protokolech můžete kopírovat do schránky vybráním daného protokolu a kliknutím na tlačítko **Kopírovat**.

10.1.1 Údržba protokolů

Nastavení protokolů ESET Cyber Security je dostupné z hlavního okna programu po kliknutí na záložku **Nastavení > Otevřít rozšířené nastavení programu... > Nástroje > Protokoly**. Zde můžete nastavit tyto parametry:

- **Automaticky mazat staré záznamy protokolů** – po zaškrtnutí této možnosti se budou automaticky odstraňovat protokoly starší než určený počet dnů,
- **Automaticky optimalizovat protokoly** – tato možnost zajišťuje defragmentaci databáze protokolů podle nastavení horního limitu množství nevyužitých záznamů v procentech.

Všechny související informace zobrazené v grafickém rozhraní, zprávy o nalezených hrozbách a událostech můžete ukládat do čitelné podoby jako plain text nebo CSV (hodnoty oddělené středníkem) soubor. Pokud si chcete tyto soubory následně prohlížet v nástrojích třetích stran vyberte možnost Zaznamenávat do textových souborů.

Pro definování cílové složky, do které chcete uložit protokoly, klikněte na tlačítko **Nastavit...** v **Rozšířeném nastavení**.

V závislosti na vybrané možnosti v **Textové protokoly: Upravit** můžete do protokolů ukládat tyto typy informací:

- Události typu *Moduly se nepodařilo aktualizovat* apod. jsou zapsány do souboru *eventslog.txt*.
- Detekované hrozby skenerem po spuštění, rezidentní ochranou nebo kontrolou počítače se zapisují do souboru *threatslog.txt*.
- Výsledky všech dokončených kontrol jsou uloženy do souboru *scanlog.ČÍSLO.txt*.

Pro konfiguraci filtrů **Standardní záznamy protokolů kontroly počítače** klikněte na tlačítko **Upravit...** a vyberte/zrušte označení u požadovaných typů záznamů. Více podrobností o protokolech naleznete v [této kapitole](#) ^[25].

10.1.2 Filtrování protokolů

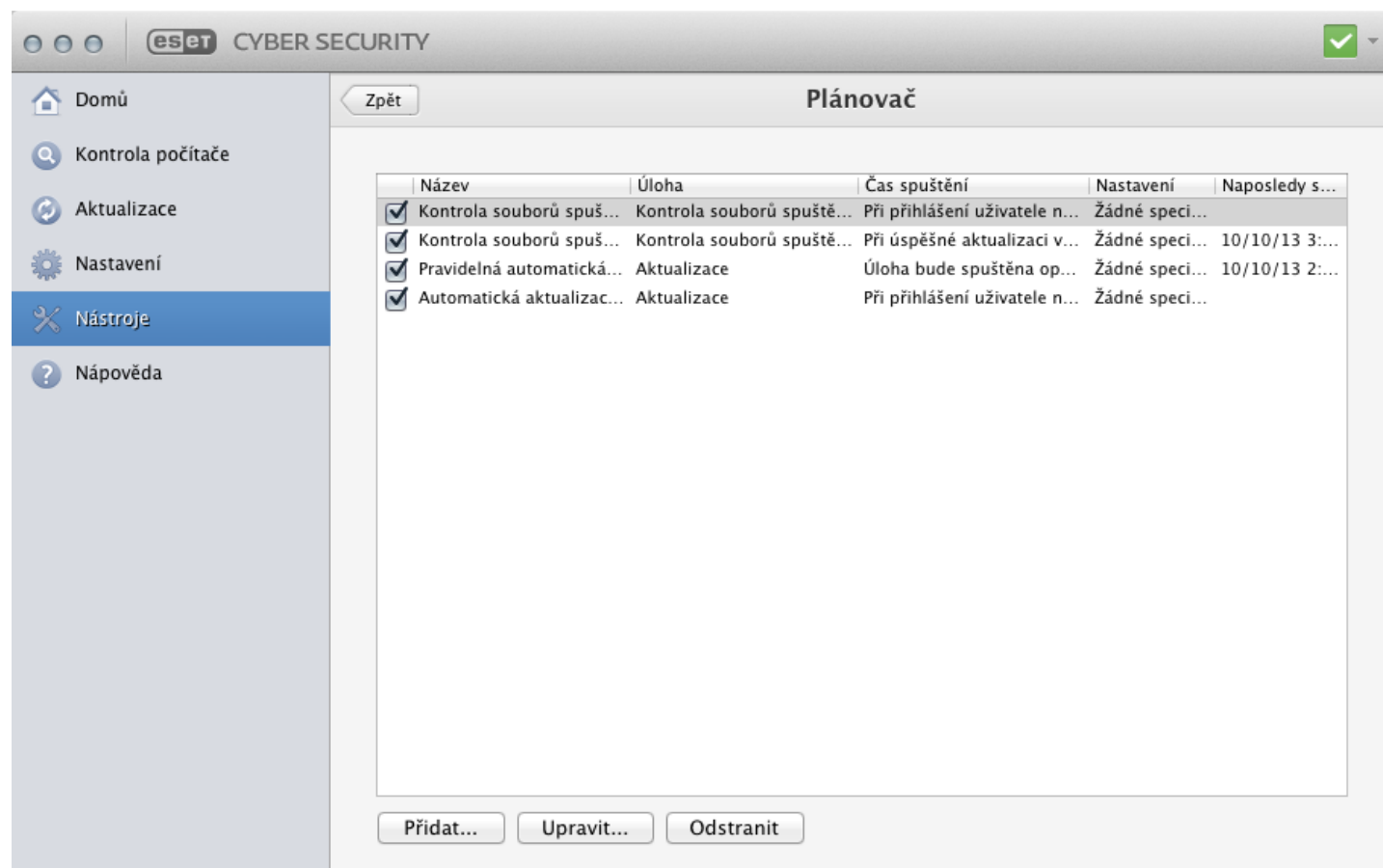
Protokoly obsahují různé druhy záznamů. Použitím filtru můžete zobrazit protokoly pouze zaznamenávající pouze záznamy specifické události.

Vybírat můžete z následujících druhů protokolů:

- **Kritická upozornění** – zaznamenány budou pouze kritické chyby systému (např. nespuštění antivirové ochrany),
- **Chyby** – zaznamenány budou chyby typu "*Chyba při stahování souboru aktualizace*" a kritická upozornění,
- **Varování** – zaznamenány budou varovné zprávy a všechny výše uvedené záznamy,
- **Informační záznamy** – zaznamenány budou informační zprávy (např. o úspěšné aktualizaci) a všechny výše uvedené záznamy,
- **Diagnostické záznamy** – zaznamenány budou informace důležité pro ladění programu a všechny výše uvedené záznamy.

10.2 Plánovač

Plánovač najdete v hlavním okně ESET Cyber Security na záložce **Nástroje**. Plánovač obsahuje seznam všech naplánovaných úloh a jejich nastavení jako je datum a čas provedení použitý profil kontroly atp.



Plánovač spravuje a spouští naplánované úlohy s nastavenými parametry a vlastnostmi. Parametry úlohy jsou datum, čas nebo jiné podmínky spuštění stejně jako profil kontroly.

Standardně se v plánovači zobrazují tyto naplánované úlohy:

- Údržba protokolů (po aktivování možnosti **Zobrazovat systémové úlohy** v nastavení Plánovače),
- Kontrola souborů spouštěných při startu počítače po přihlášení uživatele,
- Kontrola souborů spouštěných při startu počítače po úspěšné aktualizaci detekčních modulů,
- Pravidelná automatická aktualizace,
- Automatická aktualizace po přihlášení uživatele.

Pro úpravu nastavení již existující naplánované úlohy (předdefinované nebo vytvořené uživatelem) vyberte danou úlohu a klikněte na tlačítko **Upravit...** Případně stiskněte klávesu CTRL, klikněte na úlohu a vyberte možnost **Upravit...**

10.2.1 Vytvoření nové úlohy

Pokud chcete vytvořit novou úlohu v Plánovači, klikněte na tlačítko **Přidat...** nebo klikněte pravým tlačítkem kamkoli do seznamu úloh a z kontextového menu vyberete **Přidat...** Vytvořit můžete pět typů naplánovaných úloh:

- Spuštění aplikace
- Aktualizace
- Údržba protokolů
- Kontrola počítače
- Kontrola souborů spouštěných po startu

POZNÁMKA: Po vybrání možnosti **Spuštění aplikace** můžete spouštět programy jako systémový uživatel "nobody." Oprávnění pro běh aplikací spouštěným pomocí plánovače je definováno v systému macOS.

Jelikož je aktualizace jednou z nejčastěji používaných úloh, na následujícím příkladu si ukážeme přidání této úlohy do Plánovače:

1. Z rozbalovacího menu **Naplánovaná úloha** vyberte možnost **Aktualizace**.

2. Do pole **Název** úlohy zadejte název úlohy.
3. Z menu **Provedení úlohy** vyberte interval spouštění úlohy. V závislosti na nastaveném intervalu budou dostupné další volby. Pokud jako interval vyberete **Definované uživatelem**, v dalším kroku je potřeba nastavit datum a čas ve formátu cron (pro více informací se podívejte se do kapitoly [Vytvoření uživatelské úlohy](#) ^[27]).
4. V dalším kroku nastavte, jaká akce se provede v případě, že úlohu nebylo možné provést v naplánovaném čase.
5. Po nastavení všech parametrů se zobrazí souhrn vlastností naplánované úlohy a klikněte na tlačítko **Ukončit**. Nově vytvořená úloha bude přidána do plánovače a zobrazena v seznamu.

Standardně ESET Cyber Security obsahuje další důležité úlohy nutné pro správnou funkčnost. Tyto úlohy nemohou být změněny a jsou skryté. Pro zobrazení těchto úloh klikněte v hlavním okně programu na záložku **Nastavení > Otevřít rozšířené nastavení programu....** Následně klikněte na **Nástroje > Plánovač** a zaškrtněte možnost **Zobrazovat systémové úlohy**.

10.2.2 Vytvoření uživatelské úlohy

Při tvorbě uživatelem definované úlohy zadávejte datum a čas v rozšířeném cron formátu (řetězec obsahující šest polí oddělených mezerou):

minuta(0-59) hodina(0-23) den v měsíci(1-31) měsíc(1-12) rok(1970-2099) den v týdnu(0-7) (neděle = 0 nebo 7)

Příklad:

30 6 22 3 2012 4

Speciální znaky podporované v cron formátu:

- hvězdička (*) – nahrazuje všechny hodnoty v poli, např. hvězdička ve třetím poli (den v měsíci) znamená každý den
- spojovník (-) – definuje rozsah; např.: 3-9
- čárka (,) – odděluje položky v seznamu; např.: 1, 3, 7, 8
- lomítko (/) – definuje přírůstky v rozsahu; např.: 3-28/5 ve třetím poli (den v měsíci) znamená třetí den v měsíci a pak každých 5 dní.

Názvy dnů (Monday-Sunday) a měsíců (January-December) nejsou podporovány.

POZNÁMKA: Pokud definujete den v měsíci i den v týdnu, úloha se provede pouze v případě, že se obě hodnoty shodují.

10.3 Karanténa

Hlavní funkcí karantény je bezpečně uschovat infikované soubory. Soubory jsou uloženy do karantény v případě, že nemohou být léčeny, pokud není bezpečné a doporučené jejich odstranění (systémové soubory) nebo pokud byly detekovány nesprávně (tzv. falešný poplach).

Do karantény můžete také ručně přidat libovolný soubor. Tento postup je vhodný, pokud soubor vykazuje podezřelou aktivitu, ale není detekován rezidentní ochranou. Soubory v karanténě můžete následně odeslat na analýzu do virové laboratoře ESET.

Soubory uložené v karanténě můžete zobrazit v přehledné tabulce, která obsahuje datum a čas přidání souboru do karantény, cestu k původnímu umístění souboru, velikost souboru v bajtech, důvod přidání (např. přidáný uživatelem) a počet infiltrací (např. pokud se jedná o archiv obsahující více infikovaných souborů). Karanténa s uloženými soubory (*/Library/Application Support/Eset/esets/cache/quarantine*) zůstává na disku i po odinstalaci ESET Cyber Security. Soubory jsou v karanténě uloženy v bezpečném šifrovaném formátu a můžete je obnovit například v případě nesprávné detekce.

10.3.1 Vložení do karantény

ESET Cyber Security automaticky přesouvá do karantény soubory, které byly rezidentní ochranou vymazány (pokud jste tuto možnost nevypnuli v okně s upozorněním). V případě potřeby můžete kliknutím na tlačítko **Přesunout...** do karantény přesunout libovolný podezřelý soubor. K tomuto účelu můžete použít také kontextové menu karantény. Stiskněte klávesu CTRL, klikněte pravým tlačítkem do okna karantény a vyberte možnost **Přesunout....** Následně najděte soubor, který chcete vložit do karantény, a klikněte na tlačítko **Otevřít**.

10.3.2 Obnovení z karantény

Soubory z karantény můžete obnovit do svého původního umístění kliknutím na tlačítko **Obnovit**. Obnovení souboru můžete provést v okně karantény kliknutím pravým tlačítkem myši na daný soubor (při stisknutí klávese CTRL) a vybráním možnosti **Obnovit**. Kontextové menu karantény nabízí také možnosti **Obnovit do...**, pomocí které můžete soubor obnovit do jiného než původního umístění.

10.3.3 Odesílání souborů

Pokud jste do karantény umístili podezřelý soubor, který nebyl detekován, nebo pokud byl soubor naopak nesprávně označen jako infikovaný a následně umístěn do karantény, pošlete ho prosím do virové laboratoře společnosti ESET. Stiskněte klávesu CTRL, klikněte pravým tlačítkem na soubor v karanténě a z kontextového menu vyberte možnost **Odeslat soubor k analýze**.

10.4 Spuštěné procesy

Nástroj **Spuštěné procesy** zobrazuje běžící procesy ve vašem počítači a poskytuje podrobné informace o běžících procesech díky technologii ESET LiveGrid®.

- **Proces** – jméno běžícího procesu. Pro zobrazení všech běžících procesů v počítači můžete také použít nástroj Sledování aktivity, který najdete v systému macOS (*/Aplikace/Utility*).
- **Úroveň rizika** – ve většině případů určí ESET Cyber Security na základě technologie ESET LiveGrid® úroveň rizika jednotlivých objektů (souborů, procesů apod.). Úroveň rizika je vyhodnocena použitím několika heuristických metod, které zjistí charakteristiku každého objektu a váhu možné nebezpečné aktivity. Na základě těchto metod je objektu přiřazena úroveň rizika. Známé aplikace vyhodnocené jako čisté jsou označeny zeleně a jsou dále automaticky vyjmuty z kontroly počítače. Díky tomu dochází ke zrychlení rezidentní i uživatelsky spuštěné kontroly. Pokud je aplikace označena jako neznámá (žlutá), nemusí jít ještě o škodlivou aplikaci. Obvykle se jedná o novou verzi aplikace. V případě, že nedokážete sami rozhodnout, zda je aplikace škodlivá, odešlete ji na analýzu do virové laboratoře ESET. Pokud bude aplikace označena jako škodlivý kód, bude její detekce přidána do jedné z dalších aktualizací virové databáze.
- **Počet uživatelů** – množství uživatelů používající tuto aplikaci. Tato informace je poskytována technologií ESET LiveGrid®.
- **Datum nalezení** – doba, kdy byla aplikace poprvé zaznamenána technologií ESET LiveGrid®.
- **ID balíku aplikace** – jméno výrobce aplikace nebo procesu.

Pokud kliknete na některý proces, v dolní části okna se zobrazí následující informace:

- **Soubor** – umístění souboru v počítači,
- **Velikost souboru** – fyzická velikost souboru na disku,
- **Popis souboru** – popis souboru v operačním systému,
- **ID balíku aplikace** – jméno výrobce aplikace nebo procesu,
- **Verze souboru** – informace o verzi souboru od poskytovatele aplikace,
- **Název produktu** – jméno aplikace nebo její obchodní jméno.

10.5 ESET LiveGrid®

Systém včasného varování ESET LiveGrid® zajišťuje okamžité informování společnosti ESET v případě výskytu nových hrozeb. Obousměrný systém včasného varování ESET LiveGrid® má jediný účel – zlepšení ochrany, kterou vám můžeme poskytnout. Nejlepší způsob, jak zajistit, abychom věděli o nových hrozbách ihned po jejich vypuštění na internet, je spojením s našimi uživateli.

1. Pokud se rozhodnete ESET LiveGrid® nepoužívat, nepřijdete o žádnou funkcionalitu programu a ochrana vašeho počítače bude na vysoké úrovni.
2. Systém ESET LiveGrid® můžete nastavit tak, aby odesílal anonymní informace o nových hrozbách, pokud obsahují nový vzorek škodlivého kódu. Tyto informace budou poskytnuty virové laboratoři ESET, která na jejich základě může vylepšovat detekční schopnosti programu a aktualizovat detekční moduly.

ESET LiveGrid® sbírá anonymní informace z vašeho počítače přímo související s novými hrozbami. Tyto informace mohou obsahovat vzorek nebo kopii souboru, ve kterém byla zjištěna hrozba, cestu k tomuto souboru, název souboru, datum a čas, jméno procesu který k souboru přistoupil a informace o vašem operačním systému.

Žádná ze získaných informací nebude použita za jiným účelem, než je úprava detekce, schopností programu a okamžitá reakce na nové hrozby.

Pro nastavení technologie LiveGrid klikněte v hlavním okně programu na záložku **Nastavení > Otevřít rozšířená nastavení programu...** (nebo stiskněte klávesy *cmd+, > Nástroje > ESET LiveGrid®*). Vyberte volbu **Zapnout systém včasného varování** a klikněte na tlačítko **Nastavit...**

10.5.1 Odesílání podezřelých souborů

Standardně ESET Cyber Security odesílá podezřelé soubory do virové laboratoře ESET pro detailní analýzu. Pokud si nepřejete soubory posílat, odškrtněte možnost **Odeslat podezřelé soubory**.

Pokud naleznete podezřelý soubor, můžete jej okamžitě odeslat na analýzu do virové laboratoře ESET kliknutím v hlavním okně programu na **Nástroje > Odeslat soubor k analýze**. V případě, že se jedná o škodlivou aplikaci, její detekce bude přidána v další aktualizaci detekčního jádra.

Odesílat anonymní statistické informace – ESET LiveGrid® sbírá anonymní informace z vašeho počítače přímo související s novými hrozbami. Tyto informace obsahují jméno hrozby, datum a čas detekce, verzi produktu ESET, verzi operačního systému a vaši aktuální pozici. Statistické informace se většinou do laboratoře ESET odesílají dvakrát za den.

Příklad zasílané statistické informace:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/rdgFR1463[1].zip
```

Vyloučit tyto soubory – pomocí této možnosti můžete vyloučit vybrané typy souborů, které nechcete odesílat do virové laboratoře ESET. Například dokumenty a tabulky obsahující důvěryhodné informace. Standardně jsou vyloučeny soubory s příponou .doc, .rtf a další a do seznamu výjimek můžete přidat vlastní typy souborů.

Kontaktní e-mail (nepovinný údaj) – na zadané e-mailové adrese vás mohou kontaktovat specialisté z virové laboratoře ESET za účelem získání dalších informací. Pokud nejsou vyžadovány další informace, standardně nebudete kontaktováni.

11. Uživatelské rozhraní

Nastavení uživatelského rozhraní vám umožňuje upravit si pracovní prostředí programu dle vašich potřeb. Tyto možnosti naleznete v rozšířeném nastavení (dostupném z hlavního okna po stisknutí kláves `cmd+,`) v sekci **Uživatel > Rozhraní**.

- Pro zobrazování úvodního obrázku při startu ESET Cyber Security zaškrtněte možnost **Zobrazit úvodní obrázek při startu**.
- Možnost **Ponechat aplikaci v docku** zobrazí ikonu  ESET Cyber Security v macOS docku a umožní přepínání mezi ESET Cyber Security a ostatními běžícími aplikacemi stisknutím klávesy `cmd+tab`. Změna tohoto nastavení se projeví po restartu počítače.
- Možnost **Použít standardní menu** povolí používání určitých klávesových zkratk (viz kapitolu [Klávesové zkratky](#) ^[10]) a zobrazí v kontextové nabídce ESET Cyber Security menu baru položky Uživatelské rozhraní, Nastavení a Nástroje.
- Pokud chcete povolit zobrazování nápovědy pro některá tlačítka, zaškrtnete možnost **Zobrazovat nápovědu tlačítek**.
- Pro zobrazení a možnost výběru skrytých souborů ke kontrole v části **Cíle kontroly** na záložce **Kontrola počítače** zaškrtněte možnost **Zobrazovat skryté soubory**.
- Standardně se ikona  ESET Cyber Security zobrazuje v menu baru v pravém horním rohu obrazovky. Pokud nechcete tuto ikonu zobrazovat, deaktivujte možnost **Zobrazit ikonu v rozšířeném menu baru**. Změna tohoto nastavení se projeví po restartu počítače.

11.1 Upozornění a události

Sekce **Upozornění a události** nabízí možnosti pro úpravu zobrazování upozornění týkajících se hrozeb a systémových zpráv v ESET Cyber Security.

Vypnutím možnosti **Zobrazovat výstražná upozornění** se přestanou zobrazovat všechna okna s upozorněními, a proto je vhodné tuto možnost vypnout pouze v určitých situacích. Většinu uživatelů doporučujeme ponechat tuto možnost zapnutou.

Zaškrtnutím možnosti **Zobrazovat upozornění na pracovní ploše** zapnete zobrazování oken s upozorněními, které nepotřebují interakci uživatele (standardně se zobrazují v pravém horním rohu obrazovky). Pokud chcete nastavit dobu zobrazení tohoto upozornění upravte hodnotu v poli **Upozornění zavřít automaticky po X sekundách** (standardně po 5).

Od verze ESET Cyber Security 6.2 můžete potlačit zobrazování konkrétních [stavů ochrany](#) ^[30].

11.1.1 Zobrazení upozornění

ESET Cyber Security zobrazuje dialogová okna s informacemi o nových aktualizacích programových komponent, aktualizacích operačního systému a také při vypnutí určitých částí programu, vymazání protokolů apod. Potlačit zobrazování každého okna můžete kliknutím na **Příště nezobrazovat**.

Seznam dialogových oken (Nastavení > Otevřít rozšířená nastavení programu... > Upozornění a události > Nastavit...) zobrazuje seznam všech dialogových oken v ESET Cyber Security. Pro zapnutí či potlačení každého dialogu použijte přepínač vedle jména dialogového okna. Dále můžete nastavit pro některá okna různé podmínky zobrazování, např. jaké informace budou zobrazovány při dostupnosti nové verze programu nebo aktualizací operačního systému.

11.1.2 Stavy ochrany

Informace o stavu ESET Cyber Security se zobrazují v hlavním okně programu na záložce Stav ochrany. V případě potřeby můžete zobrazování konkrétních stavů ochrany potlačit. Konfiguraci jednotlivých stavů naleznete v rozšířeném nastavení (dostupném z hlavního okna po stisknutí kláves `cmd+,`) v sekci **Upozornění a události**. Následně klikněte na tlačítko **Nastavit** u položky **Zobrazit v hlavním okně na záložce Stav ochrany**.

Potlačit můžete zobrazování následujících stavů:

- Anti-Phishing je vypnutý,
- Ochrana přístupu na web je vypnutý,
- Ochrana poštovních klientů je vypnutá,
- Operační systém není aktualizovaný,
- Platnost licence se blíží ke konci,
- Platnost licence vypršela,
- Vyžadován restart systému.

11.2 Práva

Správné nastavení ESET Cyber Security může být velmi důležité pro podnikovou bezpečnost. Neoprávněné změny mohou ohrozit stabilitu a stav ochrany systému. Můžete tedy nastavit, kteří uživatelé budou mít oprávnění měnit nastavení programu.

Pro definování oprávněných uživatelů přejděte do **Nastavení > Otevřít rozšířená nastavení programu... > Oprávnění**.

Pro zajištění maximálního zabezpečení systému je důležité, aby byl program správně nastaven. Neautorizovaná změna můžete vést k ztrátě důležitých dat. Pro nastavení seznamu oprávněných uživatelů vyberte daného uživatele ze seznamu uživatelů v levé části dialogového okna **Oprávnění** a klikněte na tlačítko **Přidat**. Všechny systémové účty zobrazíte po zaškrtnutí možnosti **Zobrazit všechny uživatele**. Pro odebrání uživatele ze seznamu oprávněných uživatelů jej vyberte a klikněte na tlačítko **Odebrat**.

POZNÁMKA: Pokud ponecháte seznam oprávněných uživatelů prázdný, všichni uživatelé budou automaticky považováni za oprávněné ke změně nastavení programu.

11.3 Kontextové menu

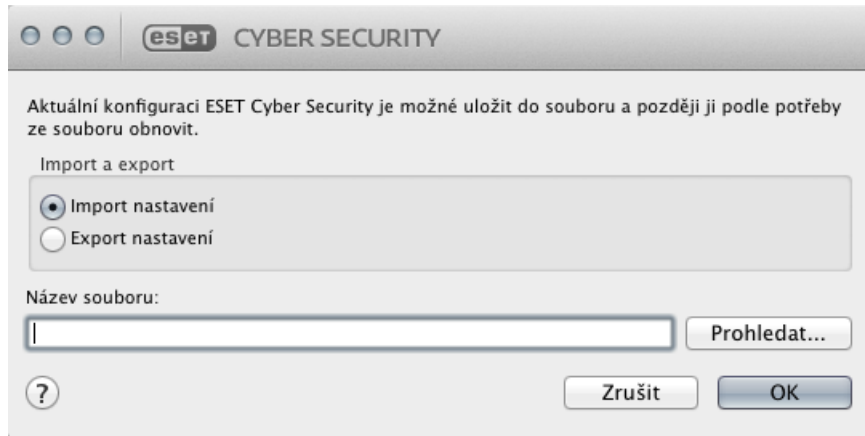
Integraci kontextového menu do systému můžete zapnout v rozšířeném nastavení (dostupném z hlavního okna po stisknutí kláves po *cmd+*) v sekci **Uživatel > Kontextové menu** po zaškrtnutí možnosti **Používat kontextové menu**. Pro provedení změn je nutné provést odhlášení uživatele nebo restartovat počítač. Možnosti kontextového menu se zobrazí, když v okně **Finder** stisknete klávesu CTRL a myší kliknete na jakýkoli soubor.

12. Různé

12.1 Import a export nastavení

Pro importování nebo exportování konfigurace ESET Cyber Security přejděte v hlavním okně na záložku **Nastavení** a klikněte na možnost **Import a export nastavení**.

Importování a exportování nastavení je užitečné například pokud si potřebujete zálohovat současné nastavení ESET Cyber Security a chcete se k němu později vrátit. Export nastavení oceníte také v případě, že chcete stejné nastavení použít na více počítačích, kdy stačí pouze naimportovat daný .xml soubor.



Pro importování nastavení vyberte možnost **Import**. Do pole **Název souboru** zadejte cestu ke konfiguračnímu souboru nebo klikněte na tlačítko **Procházet...** a požadovaný soubor vyberte ručně.

Pro exportování nastavení vyberte možnost **Export**. Klikněte na tlačítko **Procházet...**, zadejte název souboru a vyberte umístění pro uložení souboru.

12.2 Nastavení proxy serveru

Nastavení proxy serveru provedení v rozšířeném nastavení (dostupném z hlavního okna po stisknutí kláves po *cmd+*) v sekci **Různé > Proxy Server**. Tato nastavení specifikují globální nastavení proxy serveru a tyto parametry se použijí pro jakýkoliv modul ESET Cyber Security, který požádá o připojení k internetu. ESET Cyber Security podporuje Basic Access a NTLM (NT LAN Manager) způsoby autentifikace.

Po zaškrtnutí možnosti **Použít proxy server** vyplňte do pole **Proxy Server** adresu a port proxy serveru (standardně 3128).

Pokud proxy server vyžaduje autentifikaci, zatrhněte možnost **Proxy server vyžaduje autentifikaci** a vyplňte přihlašovací údaje.

13. Slovník pojmů

13.1 Typy infiltrací

Jako infiltrace je označován škodlivý software, který se snaží proniknout do počítače a vykonávat škodlivou činnost.

13.1.1 Viry

Tento druh infiltrací obvykle napadá již existující soubory na disku. Pojmenován byl podle biologického viru, protože se z počítače na další počítač šíří obdobným způsobem. Pojem vir se často nesprávně používá pro označení dalších typů hrozeb a infiltrací. Tento zaběhnutý výraz dnes nahrazuje mnohem přesnější termín "malware" (škodlivý software).

Počítačové viry napadají nejčastěji spustitelné soubory a dokumenty. Děje se to tak, že „tělo“ viru se k nim připojí – obvykle na konec souboru. Průběh aktivace počítačového viru je tedy zhruba následující: po spuštění napadeného souboru nejprve dojde ke spuštění připojeného viru. Ten vykoná akci, kterou má v sobě naprogramovanou. A až nakonec se ke slovu dostane původní aplikace. Vir může nakazit každý soubor, ke kterému má aktuálně přihlášený uživatel oprávnění pro zápis.

Vlastní činnost aktivovaného viru může mít mnoho podob. Některé viry jsou krajně nebezpečné, protože dokáží cíleně mazat soubory z disku, na druhé straně jiné mají pouze zdůraznit zručnost svých tvůrců a uživatele spíše obtěžují, než aby způsobovaly reálnou škodu.

Je potřeba říci, že viry jsou (na rozdíl od trojských koní či spyware) v dnešní době čím dál tím vzácnější, protože jsou pro své tvůrce komerčně nezajímavé. Pojem virus se často nesprávně používá pro označení všech druhů infiltrací. V současnosti se již od tohoto pojmenování upouští a prosazuje se výstižnější a správnější společný název „škodlivý kód“ (malware).

V případě infikování virem není možné napadený soubor vrátit do původní podoby, tedy vyléčit jej pomocí antivirového systému. V některých případech není možné části infikovaných souborů vyléčit a musí být nahrazeny pouze čistou kopií. Přesto jej doporučujeme odeslat do virových laboratoří společnosti ESET.

13.1.2 Červi

Počítačový červ je program obsahující škodlivý kód, který napadá hostitelské počítače a šíří se dál prostřednictvím sítě. Základní rozdíl mezi virem a červem je ten, že červ se dokáže šířit sám a není závislý na hostitelském souboru (či boot sektoru disku). Červ využívá k šíření hlavně elektronickou poštou nebo bezpečnostní zranitelnosti v síťových aplikacích.

Červ je tedy mnohem životaschopnější než virus. Díky značnému rozšíření internetu se červ dokáže dostat do celého světa během několika hodin od vydání, v některých případech dokonce v průběhu několika minut – a proto je mnohem nebezpečnější než ostatní druhy malware.

Aktivovaný červ v systému dokáže způsobit celou řadu nepříjemností – od mazání souborů, přes značné zpomalení činnosti počítače, až po deaktivaci některých programů. Díky svému charakteru je ideální pro distribuci dalších druhů infiltrací.

V případě nákazy počítače červem doporučujeme infikovaný soubor odstranit, protože obsahuje výhradně škodlivý kód.

13.1.3 Trojské koně

Dříve platilo, že trojské koně byly typem infiltrace, která se snažila maskovat za užitečné programy, aby si zajistila své spuštění uživatelem. Dnes se již takto obvykle neprezentují a jejich hlavním cílem je získat snadný přístup do systému, aby tam mohli vykonávat škodlivou činnost. Termín trojský kůň je v současnosti obecný pojem, kterým je označována v podstatě jakákoli infiltrace, kterou nelze zařadit do jiné kategorie.

Vzhledem k tomu, že se jedná o poměrně širokou kategorii aplikací, existuje řada druhů trojských koní. Mezi nejznámější patří:

- Downloader – škodlivý program, jehož úlohou je z internetu stahovat do systému další infiltrace,
- Dropper – tzv. nosič. Přenáší v sobě ukrytý další škodlivý software a ztěžuje tím jejich detekci antivirovými programy,
- Backdoor – tzv. zadní dvířka. Jedná se o program komunikující se vzdáleným útočníkem, který tak může získat přístup a kontrolu nad napadeným systémem,
- Keylogger – sleduje, jaké klávesy uživatel stisknul a odesílá informace vzdálenému útočníkovi,
- Dialer – připojuje se na zahraniční telefonní čísla, která jsou zpoplatněna vysokými částkami. Uživatel prakticky nemá šanci zaregistrovat odpojení od svého poskytovatele připojení a vytvoření nového připojení do zahraničí. Reálnou škodu mohou tyto programy způsobit pouze uživatelům s vytáčeným připojením (tzv. dial-up).

Pokud v počítači detekujete trojský kůň, doporučujeme daný soubor vymazat, protože zpravidla neobsahuje prakticky nic jiného, než samotný škodlivý kód.

13.1.4 Rootkity

Rootkit je škodlivý kód, který umožňuje získat útočníkovi neomezený přístup k počítači. Po nákaze (obvykle využití zranitelnost v systému) využívají ke svému zamaskování systémové funkce. Vydávají se za systémové procesy, soubory a složky, nebo data v registru a z tohoto důvodu je velmi těžké rootkity detekovat standardními technikami.

13.1.5 Adware

Adware je zkratka termínu „advertising-supported software“. Do této kategorie patří programy, jejichž úkolem je zobrazovat reklamy. Adware obvykle sám otevře nové vyskakovací okno (tzv. pop-up okno) s reklamou v internetovém prohlížeči nebo změni nastavení výchozí domovské stránky v internetovém prohlížeči. Používají jej často výrobci volně šiřitelných (bezplatných) programů, aby si finančně zajistili vývoj vlastní, v mnoha případech užitečné aplikace.

Adware sám o sobě nebývá škodlivý, pouze uživatele obtěžuje. Nebezpečí spočívá v tom, že často provádí sledování uživatele, podobně jako spyware.

Pokud se rozhodnete používat volně šiřitelný software, doporučujeme věnovat průběhu instalace zvýšenou pozornost. Instalační program totiž často upozorňuje na to, že se spolu s daným programem nainstaluje také adware, a zpravidla máte možnost jeho instalaci zakázat.

Některé programy ovšem bez přídavného adware není možné nainstalovat nebo bude jejich funkce omezena. Z toho vyplývá, že adware se může do systému dostat „legální“ cestou, protože s tím uživatel souhlasí. Pozornost je tedy namíště. Infikovaný soubor neobsahuje v podstatě nic jiného než samotný škodlivý kód, proto v případě infekce doporučujeme soubor vymazat.

13.1.6 Spyware

Kategorie spyware zahrnuje programy, které odesílají informace bez vědomí uživatele. Odesílány jsou různé statistické informace, jako například seznam navštěvovaných internetových stránek, seznam e-mailových adres v adresáři nebo klávesy stisknuté uživatelem.

Tvůrci těchto programů argumentují tím, že se pouze snaží zjistit potřeby nebo zájmy uživatele, aby mohli uživatelům zobrazovat cílenou reklamu. Hranice zneužitelnosti je však v tomto případě velmi nejasná a nelze zaručit, že získané informace škodlivou aplikací nebudou v budoucnosti zneužity. Údaje získané spyware programy totiž mohou obsahovat různé bezpečnostní kódy, čísla bankovních účtů a další citlivá data. Spyware se šíří společně s některými volně šiřitelnými programy, aby si jejich autoři zajistili zdroj příjmu nebo nabídli zakoupení placené verze programu. Často jste o této skutečnosti informováni během instalace a máte možnost zakoupit si placenou verzi, která spyware neobsahuje.

Příkladem volně šiřitelného software obsahujícího spyware jsou hlavně klientské aplikace sítí P2P (peer-to-peer). Zvláštní podkategorií jsou programy, které se vydávají za antispyware, přičemž samy obsahují spyware – například Spyfalcon, Spy Sheriff.

Infikovaný soubor neobsahuje v podstatě nic jiného než samotný škodlivý kód, proto infikovaný soubor doporučujeme vymazat.

13.1.7 Potenciálně zneužitelné aplikace

Existuje řada legitimních programů, které za běžných podmínek zjednodušují například správu počítačových sítí. V nesprávných rukách však mohou být zneužity k nekalým účelům. Proto ESET Cyber Security dokáže detekovat potenciální hrozby.

V převážné většině se jedná o komerční a legitimní software. Může jít například o aplikace pro zobrazení vzdálené pracovní plochy, programy pro dešifrování kódů a hesel nebo tzv. keyloggery (programy na monitorování stisknutých kláves).

13.1.8 Potenciálně nechtěné aplikace

Potenciálně nechtěné aplikace jsou programy, které sice nemusí představovat bezpečnostní riziko, ale mohou mít negativní dopad na výkon počítače. Tyto aplikace se obvykle do systému nainstalují až po souhlasu uživatele. Jejich instalací dojde k určitým změnám v chování počítačového systému oproti stavu bez instalace příslušné aplikace. Mezi tyto změny v systému patří zejména:

- zobrazování oken (pop-up, reklamy), které by se jinak nezobrazovaly,
- aktivace a spuštění skrytých procesů,
- zvýšená spotřeba systémových prostředků,
- změny výsledků vyhledávání,
- komunikace se serverem výrobce aplikace.

13.2 Typy vzdálených útoků

Existují různé techniky, které umožňují útočníkům napadnout vzdálené počítače. Podle povahy se útoky dělí do několika skupin.

13.2.1 DoS útoky

DoS neboli Denial of Service – odmítnutí služby, je způsob útoku, který způsobí, že prostředky počítače nebudou dostupné pro původní uživatele. Komunikace mezi uživateli je přetížená, neprobíhá správně a pro obnovení funkčnosti je nutné počítač restartovat.

Cílem se stávají nejčastěji webové servery, kdy účelem útoku je vyřadit je z provozu.

13.2.2 DNS Poisoning

DNS Poisoning („otrávení“ pomocí odpovědi serveru DNS) je metoda, která dokáže oklamat počítač tím, že mu útočník podsuně klamné informace o DNS serveru, které považuje za autentické. Nepravdivé informace počítač určitou dobu uchovává v mezipaměti, což útočníkovi umožňuje manipulaci s DNS odpověďmi z konkrétní IP adresy. Tím dokáže u uživatele vyvolat dojem, že navštěvuje legitimní internetovou stránku, ve skutečnosti mu však může být podsunut škodlivý obsah nebo se tímto způsobem do počítače stáhne počítačový vir nebo červ.

13.2.3 Skenování portů

Skenování portů se používá v případě, kdy je třeba zjistit, které porty jsou otevřené. Port scanner je nástroj pro zjištění otevřených portů.

Počítačový port je virtuální bod, který zpracovává příchozí a odchozí data - je to klíčový bod z hlediska bezpečnosti počítače. Ve velkých sítích pomáhají informace získané pomocí port scanneru zjistit potenciální slabiny. Takové použití je legální.

Skenování portů je ale často využíváno hackery, kteří se snaží narušit bezpečnost. Prvním krokem je poslání datového paketu na každý port. V závislosti na typu odpovědi je pak možné určit, které porty jsou využívány a jsou otevřené. Skenování samo o sobě nepředstavuje riziko, ale umožňuje hackerům odhalit potenciální slabiny systému a převzít kontrolu nad vzdáleným počítačem.

Síťovým administrátorům doporučujeme všechny nevyužívané porty a otevřené porty chránit před neoprávněným přístupem.

13.2.4 Desynchronizace TCP

Desynchronizace protokolu TCP je technika využívána při tzv. útocích TCP Hijacking. Desynchronizace je vyvolána procesem, kdy se sekvenční číslo přijatého paketu neshoduje s očekávaným sekvenčním číslem. V závislosti na sekvenčním čísle poté dojde k zahození paketu (případně k jeho uložení do vyrovnávací paměti, pokud se nachází v aktuálním okně komunikace).

Ve stavu desynchronizace si obě strany v komunikaci navzájem zahazují pakety. Do toho může vstoupit útočník (sledující danou komunikaci) a dodat pakety se správným sekvenčním číslem. Útočník může v takovém případě přidávat do komunikace příkazy nebo ji jinak pozměnit.

Cílem útoku je narušit spojení na úrovni klient-server, nebo P2P komunikaci. Zabránit takovému útoku je možné použitím autentifikace jednotlivých segmentů protokolu TCP nebo dodržováním doporučených nastavení pro správu a nastavení síťových zařízení.

13.2.5 SMB Relay

SMBRelay a SMBRelay2 jsou speciální programy, které dokáží provést útok na vzdálený počítač. Program využívá protokol pro sdílení souborů SMB (Server Message Block) provázaný s rozhraním NetBIOS. Pokud sdílíte složku nebo disk v rámci lokální sítě, využíváte s nejvyšší pravděpodobností tento způsob sdílení.

V rámci komunikace uvnitř lokální sítě poté dochází k výměně kontrolních součtů (hash) uživatelských hesel.

Program SMBRelay zachytává komunikaci na portu UDP 139 a 445, přesměruje pakety mezi klientem a serverem příslušné stanice a upraví je. Po připojení a autentifikaci je klientská stanice odpojena a program SMBRelay vytvoří novou virtuální IP adresu. K této adrese se poté lze připojit příkazem „net use \\192.168.1.1“ a adresa může být používána všemi integrovanými síťovými funkcemi systému Windows. Program přenáší veškerou komunikaci SMB kromě vyjednávání (negotiation) a autentifikace. Pokud je klientský počítač připojen, vzdálený útočník se může kdykoli připojit na uvedenou IP adresu.

Program SMBRelay2 pracuje na stejném principu, místo IP adres však používá názvy z rozhraní NetBIOS. Oba programy umožňují útoky typu „man-the-middle“ (člověk uprostřed), tedy útoky, kde útočník dokáže číst, zadávat a měnit odkazy mezi dvěma stranami bez toho, aby o tom některá ze stran věděla. Nejčastějším příznakem je, že systém přestane reagovat, nebo dojde k náhlému restartování počítače.

Doporučenou ochranou proti těmto útokům je používání autentifikace za pomoci hesel nebo klíčů.

13.2.6 Útoky ICMP

Protokol ICMP (Internet Control Message Protocol) je jedním z hlavních internetových protokolů. Slouží k odesílání různých chybových hlášení a využívají ho k tomuto účelu zejména počítače a další zařízení v síti.

Útoky vedené protokolem ICMP zneužívají jeho slabá místa. ICMP je navržen pro jednosměrnou komunikaci bez ověřování. Tento fakt dovoluje vzdálenému útočníkovi vyvolat například tzv. DoS útok (Denial of Service) nebo útoky, které umožní sledování a přístup k paketům celé komunikace.

Typickými příklady ICMP útoků jsou ping flood, ICMP_ECHO flood nebo smurf attack. Mezi příznaky patří značné zpomalení internetových aplikací případně další problémy s připojením k internetu.

13.3 Elektronická pošta

Elektronická pošta, tedy e-mail přináší jako moderní forma komunikace spoustu výhod. Je flexibilní, rychlá a přímá, a byla vlastně hlavním důvodem, proč se internet v první polovině devadesátých let minulého století rozšířil po celém světě.

Bohužel díky vysoké míře anonymity vznikl prostor pro zneužívání internetu a elektronické pošty k nelegálním účelům a šíření nevyžádané pošty. Nevyžádaná pošta je poměrně širokou kategorií zahrnující například reklamy, fámy a šíření škodlivého software (malware). Nebezpečí umocňuje fakt, že náklady na rozesílání jsou v podstatě nulové a tvůrci mají k dispozici spoustu nástrojů a zdrojů na zjištění nových e-mailových adres. Množství nevyžádané pošty se tím stává těžko regulovatelné a běžný uživatel elektronické pošty je v podstatě neustále vystavován nebezpečným útokům. Čím déle je e-mailová schránka používána, tím se zvyšuje pravděpodobnost, že se dostane do databáze tvůrců nevyžádané pošty. Několik tipů na prevenci:

- pokud je to možné, nezveřejňujte svou e-mailovou adresu na internetu,
- poskytněte svoji e-mailovou adresu co nejméně,
- používejte ne zcela běžné aliasy – složitější aliasy jsou obtížněji zjistitelné technikami používanými při rozesílání nevyžádané pošty,
- neodpovídejte na nevyžádanou poštu, kterou jste obdrželi,
- věnujte pozornost vyplňování formulářů na internetu – zejména automaticky zaškrtnutým možnostem typu "Ano, chci dostávat do své schránky informace o novinkách",
- používejte více "specializovaných" e-mailových adres – např. pracovní e-mail, e-mail pro komunikaci s přáteli a další,
- jednou za čas změňte e-mailovou adresu,
- používejte antispamové řešení.

13.3.1 Reklamy

Reklama na internetu patří mezi nejrychleji rostoucí formy reklamy. Nabídky zasílané prostřednictvím e-mailu jsou jednou z forem internetové reklamy. Jejich hlavní výhodou jsou téměř nulové náklady, přímé a okamžité doručení adresátovi. Mnoho společností se snaží tímto způsobem udržovat kontakt se svými stávajícími zákazníky, případně získávat nové, protože se jedná o účinný marketingový nástroj.

Reklama zasílaná e-mailem je sama o sobě legitimní. Uživatel může mít zájem získávat reklamní informace z určité oblasti. Často si však nepřeje, aby mu reklama byla zasílána, ale přesto se tak děje. V takovém případě se reklamní e-mail stává zároveň nevyžádanou poštou – spamem.

V současné době se množství nevyžádaných reklamních e-mailů stalo velkým problémem. Tvůrci nevyžádané pošty se přirozeně snaží spam maskovat jako legitimní zprávu.

13.3.2 Fámy

Fáma (z anglického "hoax") je internetem masově šířena zpráva. Nejčastějším médiem je elektronická pošta, případně komunikační nástroje typu ICQ a Skype. Jedná se buď o falešnou poplašnou zprávu, žert, nebo mystifikaci – zpráva sama o sobě se nezakládá na pravdě.

Mezi často rozšířené fámy patří například informace o novém počítačovém viru, který má běžné (vymazání souborů, získávání hesel), nebo až přímo absurdně znějící schopnosti a snaží se vyvolat v uživateli strach.

U některých poplašných zpráv se snaží autoři zajistit co největší rozšíření zprávy výzvami na další přeposlání pod různými záminkami. Časté jsou fámy o mobilních telefonech, prosby o pomoc, nabídky na velké částky peněz ze zahraničí. Ve většině případů je obtížné zjistit původní záměr autora.

V zásadě platí pravidlo, že pokud zpráva obsahuje výzvu k dalšímu hromadnému rozesílání, jedná se s největší pravděpodobností o hoax. Na internetu existuje několik specializovaných stránek s databází fám (hoaxů), na kterých si ověřte pravost takové zprávy předtím, než ji přepošlete dále.

13.3.3 Phishing

Pojem phishing definuje kriminální činnost využívající tzv. sociální inženýrství (technika manipulace s uživateli vedoucí k získávání důvěrných informací). Cílem je získat citlivé údaje, jako například hesla k bankovním účtům, PIN kódy a jiné detaily.

Phishingem označujeme falešný e-mail tvářící se důvěryhodně, který se snaží vzbudit dojem, že jeho odesílatelem je například banka nebo pojišťovna. Grafický vzhled zprávy, nebo stránka, na kterou zpráva odkazuje, je na první pohled nerozeznatelná od té, kterou instituce používá. Pod různými záminkami, například ověření přístupových údajů, zaslání částky peněz na účet atd. jsou od uživatelů získány důvěrné informace. Ty mohou být později zneužity v neprospěch poškozeného.

Nejlepší obranou proti phishingu je na takové zprávy vůbec neodpovídat. Banky a další instituce od vás prostřednictvím e-mailu nebudou nikdy vyžadovat uživatelské jméno a heslo.

13.3.4 Rozpoznání nevyžádané pošty

Existuje několik znaků, podle kterých se dá rozpoznat, zda je přijatá e-mailová zpráva nevyžádanou poštou. Pokud daná zpráva splňuje některou z následujících podmínek, jedná se pravděpodobně o nevyžádanou poštu – spam.

- Adresa odesílatele nepatří do vašeho seznamu kontaktů.
- Dostanete výhodnou finanční nabídku, ale žádá se od vás vstupní poplatek.
- Pod různými záminkami (ověření údajů, přesun financí) jsou od vás požadovány citlivé přístupové údaje (např. číslo bankovního účtu, heslo do internetového bankovníctví apod.).
- Zpráva je napsána v cizím jazyce.
- Zpráva nabízí produkt, o který se nezajímáte. Pokud máte přece jen o produkt zájem, je vhodné si ověřit přímo u výrobce, zda odesílatel zprávy patří mezi důvěryhodné distributory.
- Zpráva obsahuje zkomolená slova, aby oklamala filtry pro nevyžádanou poštu. Například místo "viagra" ve zprávě bude "vaigra" a podobně.